Convalida del problema di produzione di CX Cloud Agent Overview v2.2. Ignorare questo articolo

Sommario

Introduzione

Questo documento descrive Cisco's Customer Experience (CX) Cloud Agent.

Prerequisiti

CX Cloud Agent viene eseguito come macchina virtuale (VM) e può essere scaricato come OVA (Open Virtual Appliance) o VHD (Virtual Hard Disk).

Requisiti

Requisiti da distribuire:

- Uno dei seguenti hypervisor:
  - VMware ESXi versione 5.5 o successiva
  - Oracle Virtual Box 5.2.30 o successivo
  - Windows Hypervisor versione 2012-2022
- L'hypervisor può ospitare una VM che richiede:
  - 8 core di CPU
  - 16 GB di memoria/RAM
  - 200 GB di spazio su disco
- Per i clienti che utilizzano i centri dati statunitensi designati come area dati principale per l'archiviazione dei dati del cloud CX, l'agente cloud CX deve essere in grado di connettersi ai server mostrati qui, utilizzando il nome di dominio completo (FQDN) e utilizzando HTTPS sulla porta TCP 443:
  - FQDN: agent.us.csco.cloud
  - FQDN: ng.acs.agent.us.csco.cloud

    - FQDN: cloudsso.cisco.com
    - FQDN: api-cx.cisco.com
- Per i clienti che utilizzano i centri dati europei designati come area dati principale per l'archiviazione dei dati del cloud CX: l'agente cloud CX deve essere in grado di connettersi a entrambi i server mostrati qui, utilizzando il nome di dominio completo (FQDN) e utilizzando HTTPS sulla porta TCP 443:
    - FQDN: agent.us.csco.cloud
    - FQDN: agent.emea.cisco.cloud
    - FQDN: ng.acs.agent.emea.cisco.cloud
    - FQDN: cloudsso.cisco.com
    - FQDN: api-cx.cisco.com
- Per i clienti che utilizzano i centri dati dell'Asia Pacifico designati come area dati principale per l'archiviazione dei dati del cloud CX: l'agente cloud CX deve essere in grado di connettersi a entrambi i server mostrati qui, utilizzando il nome di dominio completo (FQDN) e utilizzando HTTPS sulla porta TCP 443:
    - FQDN: agent.us.csco.cloud
    - FQDN: agent.apjc.cisco.cloud
    - FQDN: ng.acs.agent.apjc.cisco.cloud
    - FQDN: cloudsso.cisco.com
    - FQDN: api-cx.cisco.com
- Per i clienti che utilizzano i centri dati designati per l'Europa e l'Asia Pacifico come regione dati principale, la connettività all'FQDN: agent.us.csco.cloud è richiesta solo per la registrazione dell'agente cloud CX con CX Cloud durante la configurazione iniziale. Una volta completata la registrazione dell'agente di CX Cloud con CX Cloud, questa connessione non è più necessaria.
- Per la gestione locale dell'agente cloud CX, la porta 22 deve essere accessibile.
- In questa tabella viene fornito un riepilogo delle porte e dei protocolli che devono essere aperti e abilitati per il corretto funzionamento dell'agente cloud CX:

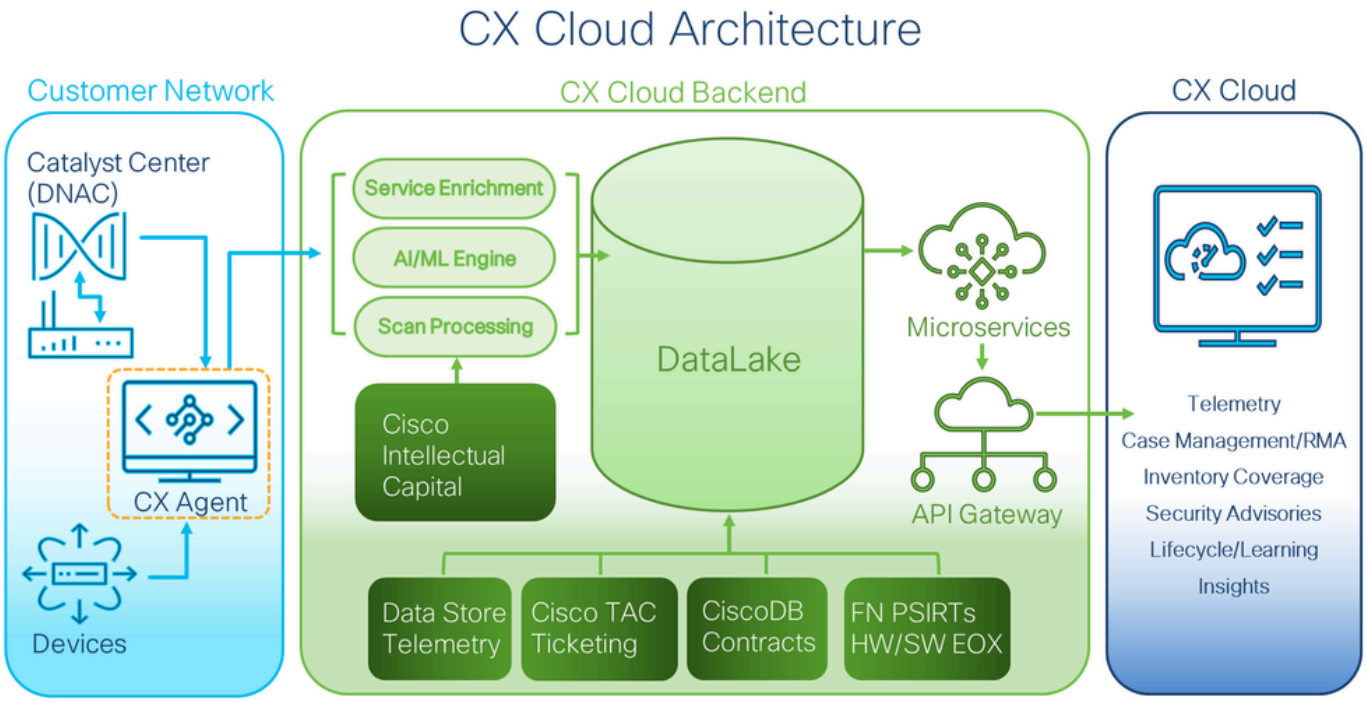
					Required for both Cisco DNA Center and Other Assets collected by CX Cloud Agent support	
					Mandatory TCP/7 Echo (ICMP) port must be combined with one of the other two ports (for device discovery process)	
CX Cloud Agent Traffic					Mandatory for other assets collected by CX Cloud Agent support	
Source	**Destination**		**Protocol**	**Port**	**Purpose**	**Type**
	IP Address	**Hostname**				
Data Collection and Transfer						
Agent IP	Dynamic IPs Cisco DNA Center Server IP	For All regions, FQDN: cloudsso.cisco.com FQDN: api-cx.cisco.com QDN: agent.us.csco.cloud DNAC Servers Additionally, For Americas region, FQDN: ng.acs.agent.us.csco.cloud For EMEA region, FQDN: agent.emea.csco.cloud, and FQDN: ng.acs.agent.emea.csco.cloud For APJC region, FQDN: agent.apjc.csco.cloud, and FQDN: ng.acs.agent.apjc.csco.cloud	HTTPS	TCP/ 443	Data collection via DNAC servers, Data transfer to CX Cloud, including upgrade functionality	Outbound connection to DNAC servers + Outbound to Cisco AWS regional data centers
Agent IP	Customer Device		SNMP	UDP/161	Collect OIDs and MIBs for other assets collected by CX Cloud Agent	Outbound to LAN
Devices	Agent IP		SYSLOG	UDP/514	Stream Syslog messages from Device to Agent	Inbound from LAN
Agent IP	Customer Device		SSH	TCP/22	Collect CLI commands	Outbound to LAN
Agent IP	Customer Device		Echo	TCP/7	Check the device reachability	Outbound to LAN
Agent IP	Customer Device		Telnet	TCP/23	Collect CLI commands	Outbound to LAN
Agent Administration Access						
Support VM	Agent IP		SSH	TCP/22	Agent Maintenance	Inbound from LAN

Premesse

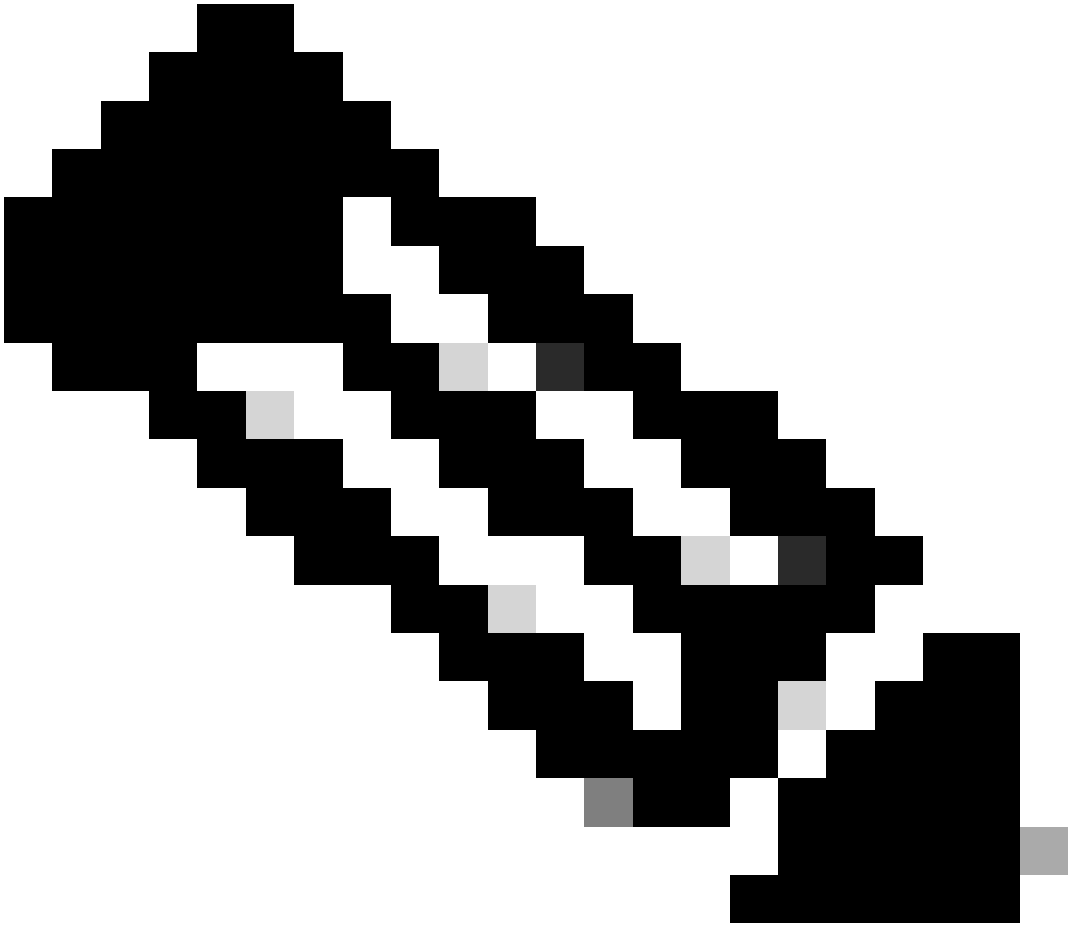
Cisco (CX) Cloud Agent è una piattaforma altamente scalabile che raccoglie dati di telemetria dai dispositivi di rete dei clienti per fornire informazioni pratiche ai clienti. CX Cloud Agent consente di

trasformare l'intelligenza artificiale (AI)/Machine Learning (ML) dei dati di configurazione in esecuzione attiva in informazioni proattive e predittive visualizzate in CX Cloud.

Questa guida è specifica di CX Cloud Agent v2.2 e versioni successive. Per accedere alle versioni precedenti, consultare la pagina Cisco CX Cloud Agent.



Architettura di CX Cloud



Nota: le immagini (e il contenuto al loro interno) in questa guida sono solo a scopo di riferimento. Il contenuto effettivo può variare.

- Se nell'ambiente VM è abilitato il protocollo DHCP (Dynamic Host Configuration Protocol), viene rilevato automaticamente un indirizzo IP. In caso contrario, devono essere disponibili un indirizzo IPv4, una subnet mask, l'indirizzo IP del gateway predefinito e l'indirizzo IP del server DNS (Domain Name Service).
- Solo IPv4 è supportato.
- Le versioni certificate di Cisco DNA Center per cluster a nodo singolo e ad alta disponibilità (HA) sono comprese tra 2.1.2.x a 2.2.3.x, 2.3.3.x, 2.3.5.x e di Cisco Catalyst Center Virtual Appliance e Cisco DNA Center Virtual Appliance.
- Se la rete dispone di un'intercettazione SSL, autorizzare-elencare l'indirizzo IP dell'agente cloud CX.
- Per tutti gli asset con connessione diretta, è richiesto il livello di privilegio SSH 15.
- Utilizzare solo i nomi host forniti. Impossibile utilizzare indirizzi IP statici.

Accesso ai domini critici

Per iniziare il percorso di CX Cloud, gli utenti devono accedere a questi domini. Utilizzare solo i nomi host forniti. Non utilizzare indirizzi IP statici.

Domini specifici del portale agenti cloud CX

Domini principali	Altri domini
cisco.com	mixpanel.com
csco.cloud	cloudfront.net
split.io	eum-appdynamics.com
	appdynamics.com
	tiqcdn.com
	jquery.com

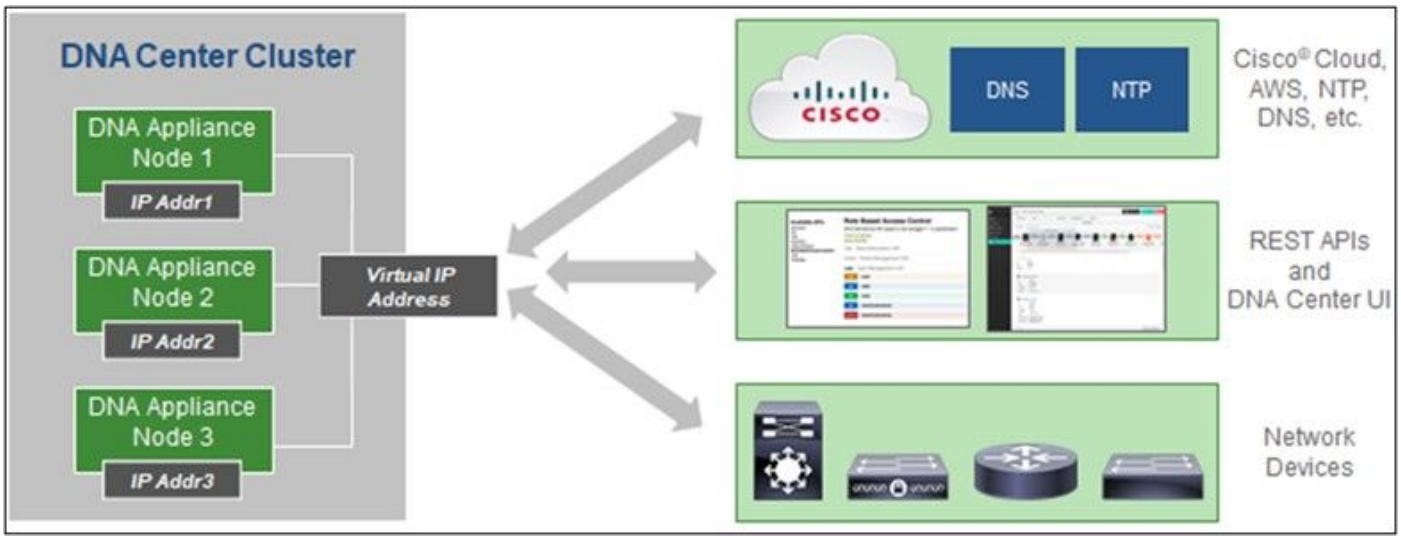
Domini specifici per l'agente cloud CX

AMERICAS	EMEA	APJC
cloudsso.cisco.com	cloudsso.cisco.com	cloudsso.cisco.com
api-cx.cisco.com	api-cx.cisco.com	api-cx.cisco.com
agent.us.csco.cloud	agent.us.csco.cloud	agent.us.csco.cloud
ng.acs.agent.us.csco.cloud	agente.emea.cisco.cloud	agente.apjc.cisco.cloud
	ng.acs.agent.emea.cisco.cloud	ng.acs.agent.apjc.cisco.cloud

Nota: l'accesso in uscita deve essere consentito con il reindirizzamento abilitato sulla porta 443 per i nomi di dominio completo (FQDN) specificati.

Versione supportata di Cisco DNA Center

Le versioni supportate di Cisco DNA Center a nodo singolo e cluster HA sono comprese tra 2.1.2.x a 2.2.3.x, 2.3.3.x, 2.3.5.x e di Cisco Catalyst Center Virtual Appliance e Cisco DNA Center Virtual Appliance.



Cisco DNA Center con cluster HA a più nodi

Browser supportati

Per un'esperienza ottimale sul sito Cisco.com, si consiglia l'ultima versione ufficiale di questi browser:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

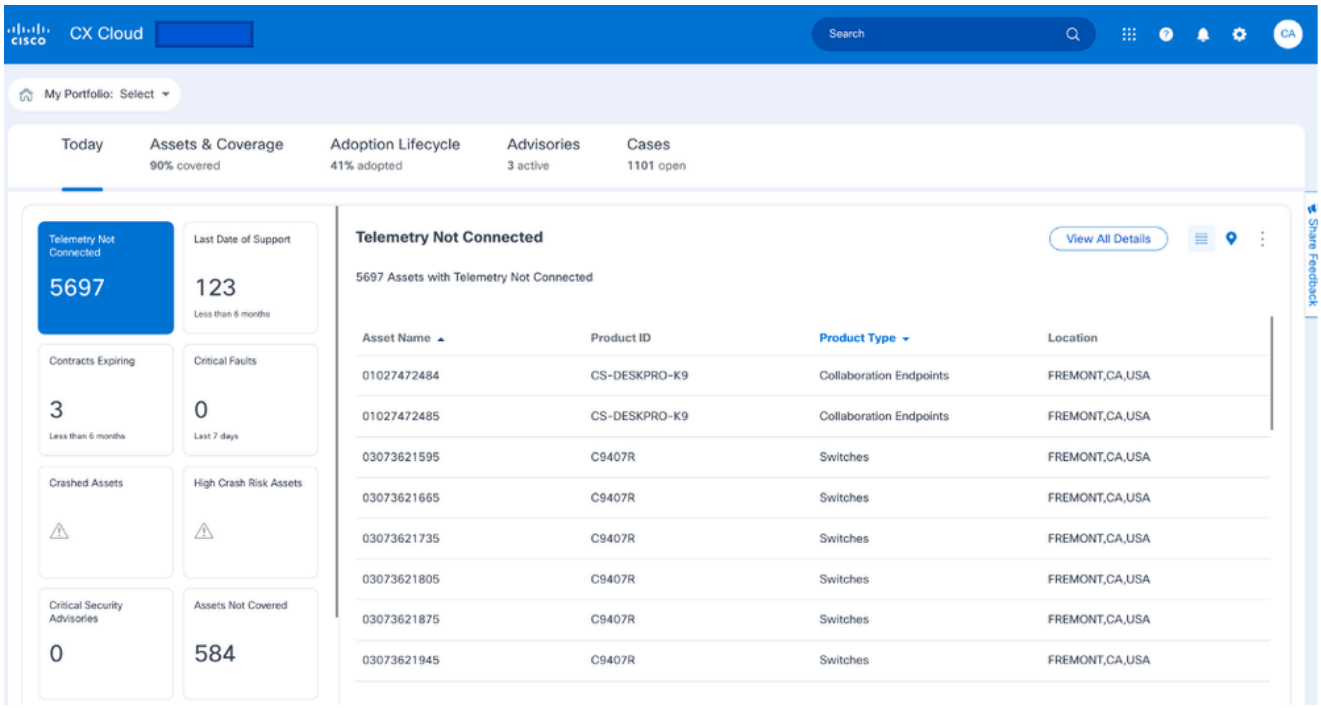
Elenco dei prodotti supportati

Per visualizzare l'elenco dei prodotti supportati da CX Cloud Agent, fare riferimento all'elenco dei prodotti supportati.

Connessione di origini dati

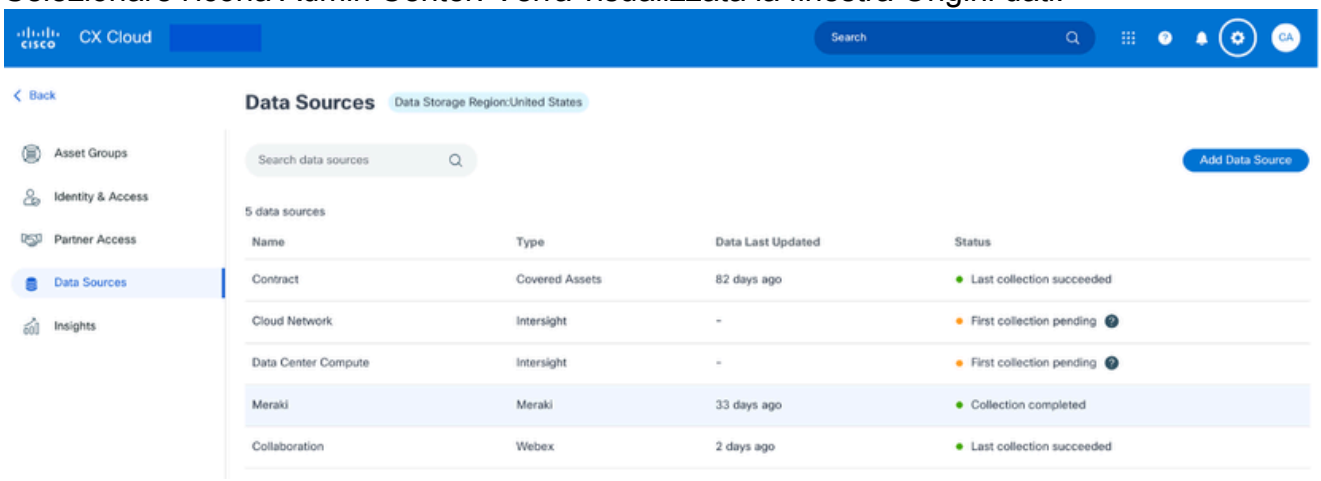
Per connettere le origini dati:

1. Fare clic su cx.cisco.com per accedere a CX Cloud.



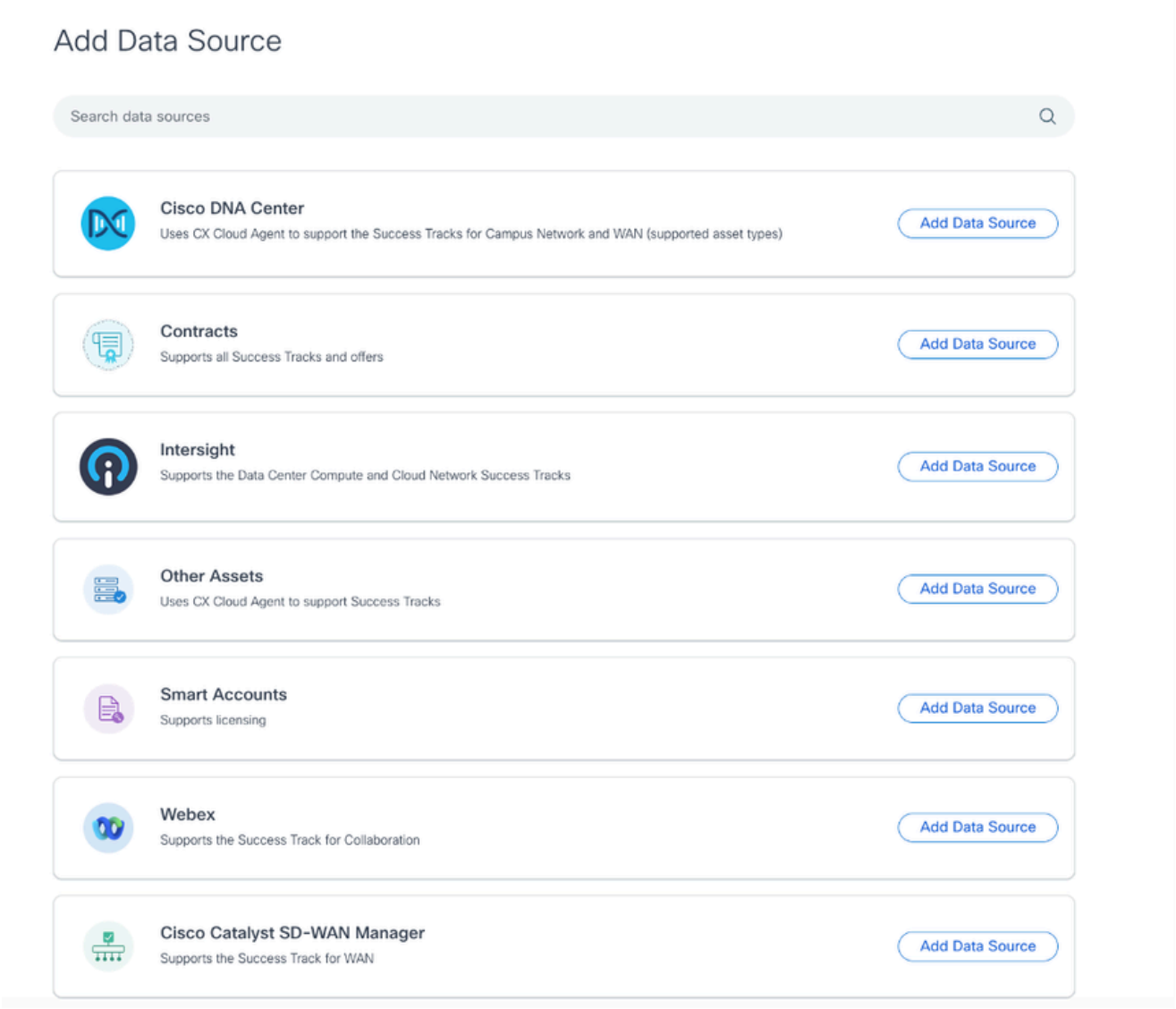
Home page di CX Cloud

2. Selezionare l'icona Admin Center. Verrà visualizzata la finestra Origini dati.



Origini dei dati

3. Fare clic su Aggiungi origine dati. Verrà visualizzata la finestra Aggiungi origine dati. Le opzioni visualizzate possono variare in base alle sottoscrizioni dei clienti.



Aggiungi origine dati

4. Fare clic su Aggiungi origine dati per selezionare l'origine dati applicabile. Se l'agente cloud CX non è stato precedentemente configurato, viene visualizzata la finestra Impostazione agente cloud CX in cui è necessario completare la configurazione. Se l'impostazione è completa, la connessione continua. Per continuare, fare riferimento a una delle sezioni seguenti:

Configurazione dell'agente cloud CX

Aggiunta di Cisco DNA Center come origine dati

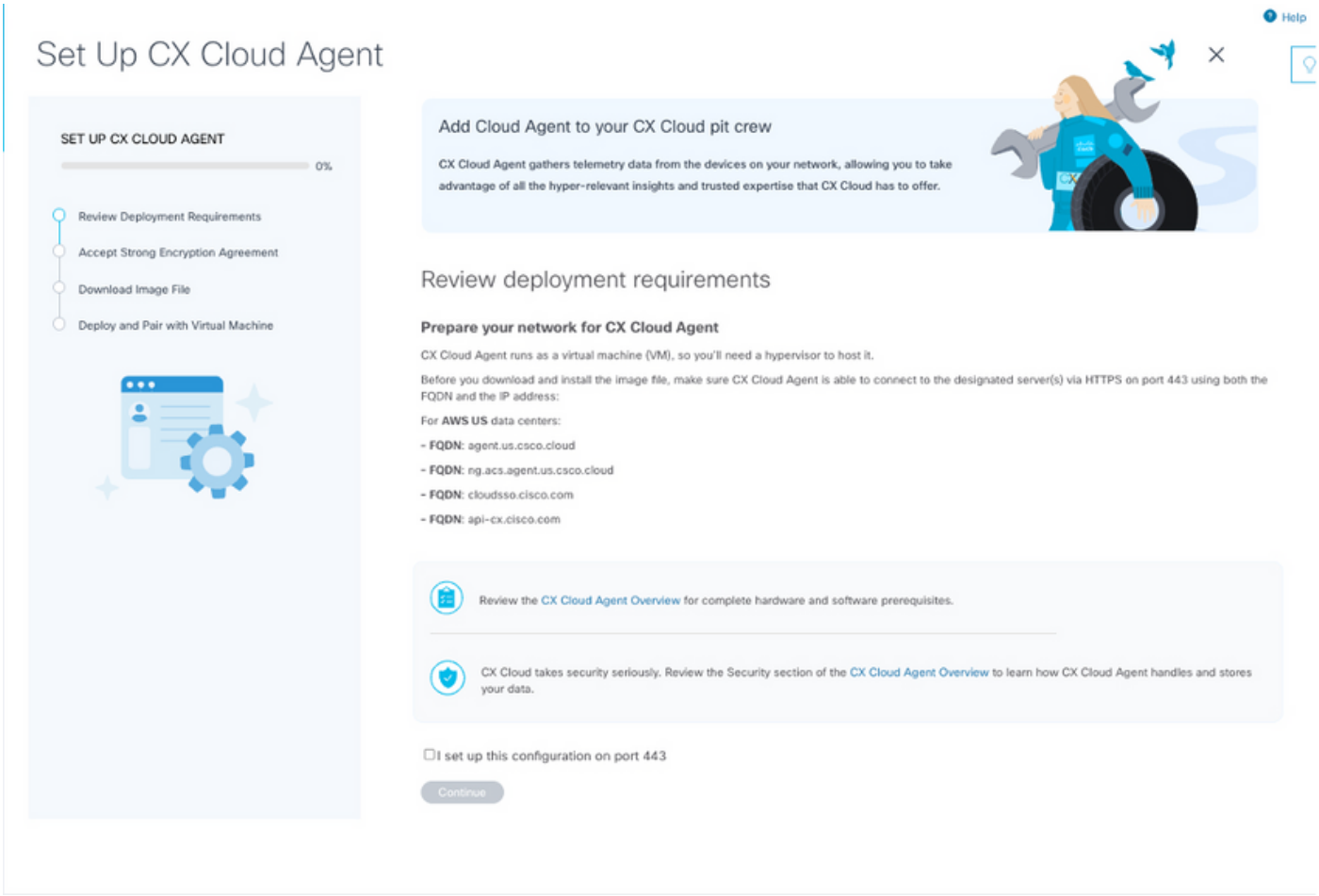
Aggiunta di altri cespiti come origini dati

Nota: l'opzione Altre risorse è disponibile solo se non è stata configurata in precedenza la connettività dei dispositivi diretti.

Configurazione dell'agente cloud CX

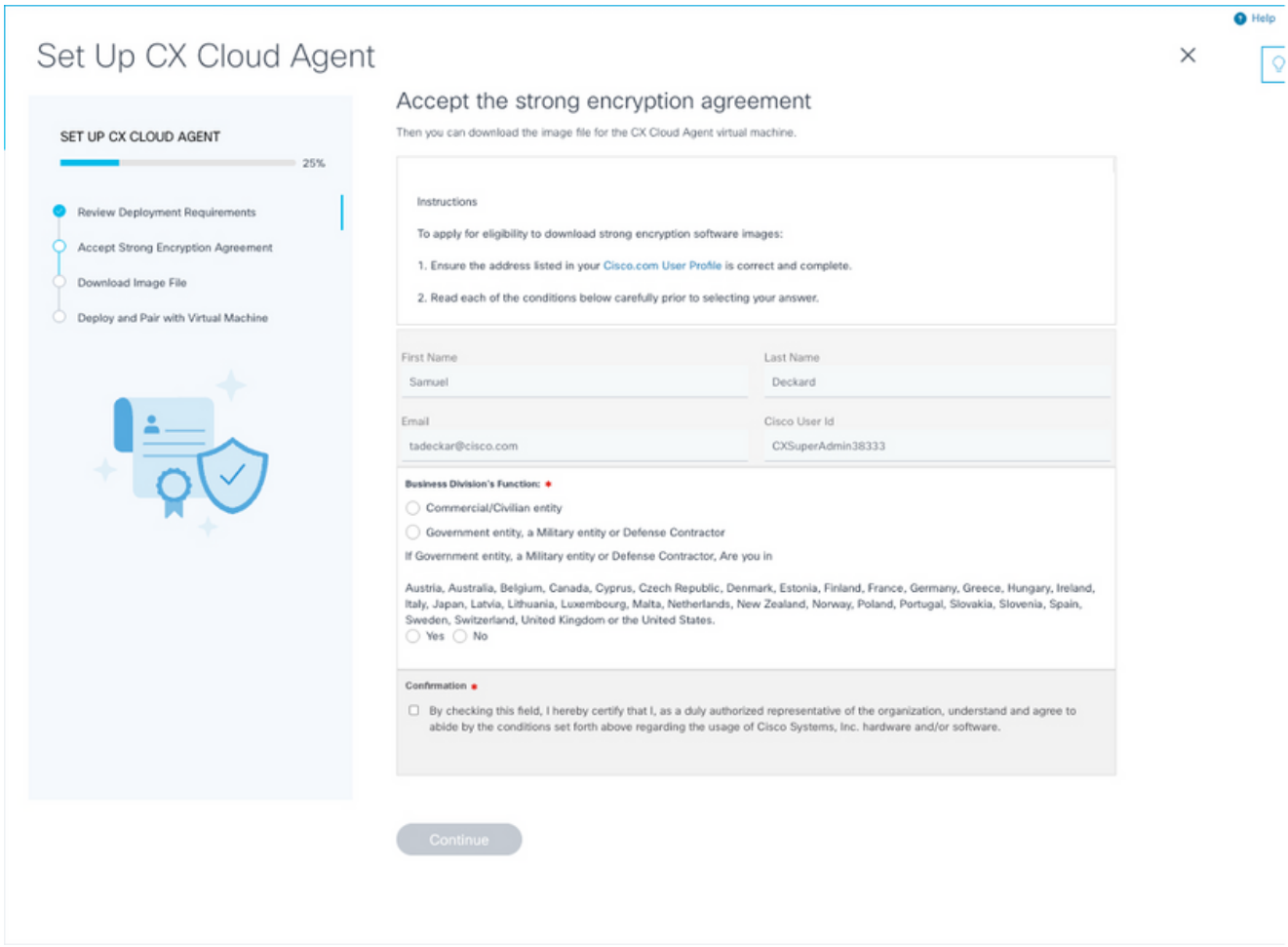
L'installazione di CX Cloud Agent viene richiesta quando si connettono le origini dati se non è stata completata in precedenza.

Per configurare l'agente cloud CX:



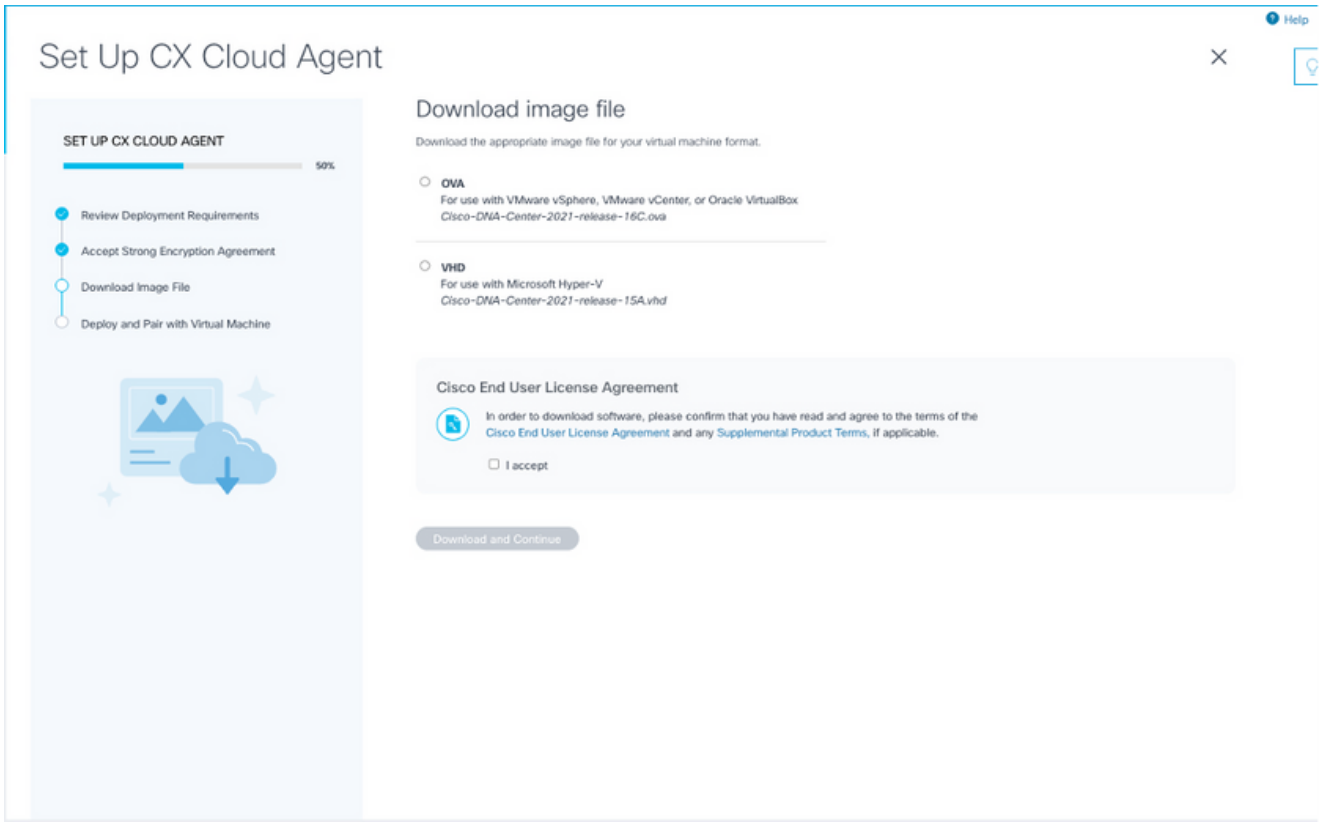
Verifica requisiti di distribuzione

1. Esaminare i requisiti di distribuzione e selezionare la casella di controllo I set up this configuration on port 443.
2. Fare clic su Continue (Continua). Viene visualizzata la finestra Set Up CX Cloud Agent - Accept the strong encryption agreement.



Contratto di crittografia

3. Verificare le informazioni precompilate nei campi Nome, Cognome, Posta elettronica e ID utente Cisco.
4. Selezionare la funzione della divisione aziendale appropriata.
5. Selezionare la casella Confirmation (Conferma) e accettare le condizioni di utilizzo.
6. Fare clic su Continue (Continua). Viene visualizzata la finestra Set Up CX Cloud Agent - Download image file (Imposta agente cloud CX - Scarica file immagine).



Scarica immagine

7. Selezionare il formato di file appropriato per scaricare il file di immagine necessario per l'installazione.
8. Selezionare la casella di controllo Accetto per accettare il contratto di licenza con l'utente finale Cisco.
9. Fare clic su Download e Continua. Viene visualizzata la finestra Configura agente cloud CX - Distribuisci e associa alla macchina virtuale.
10. Per ottenere il codice di associazione richiesto nella sezione successiva, consultare Configurazione di rete.

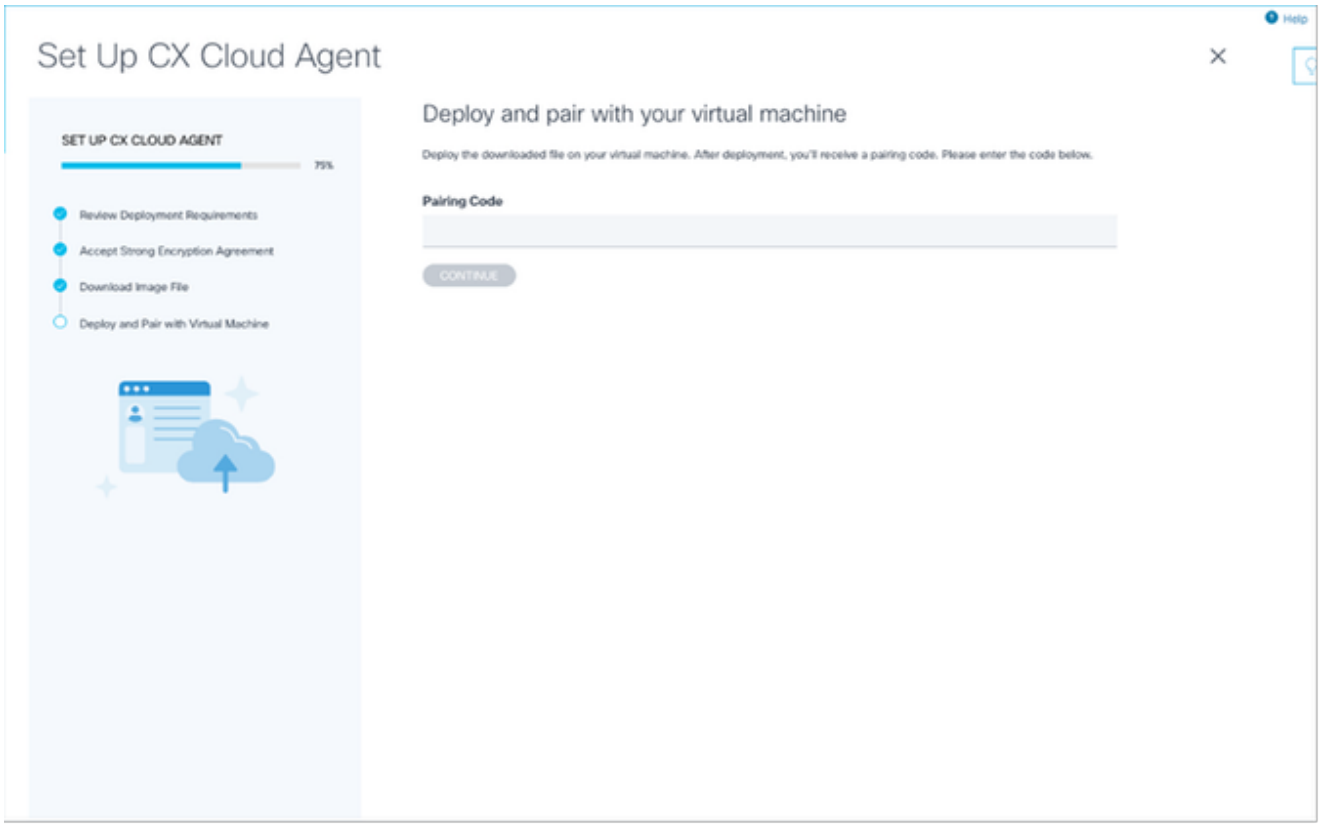
Connessione di CX Cloud Agent a CX Cloud

La connessione dell'agente di CX Cloud a CX Cloud è necessaria per l'avvio della raccolta di telemetria, in modo che le informazioni nell'interfaccia utente possano essere aggiornate per visualizzare le risorse correnti e le informazioni dettagliate. In questa sezione vengono fornite informazioni dettagliate per completare le linee guida per la connessione e la risoluzione dei problemi.

Per connettere l'agente di CX Cloud a CX Cloud:

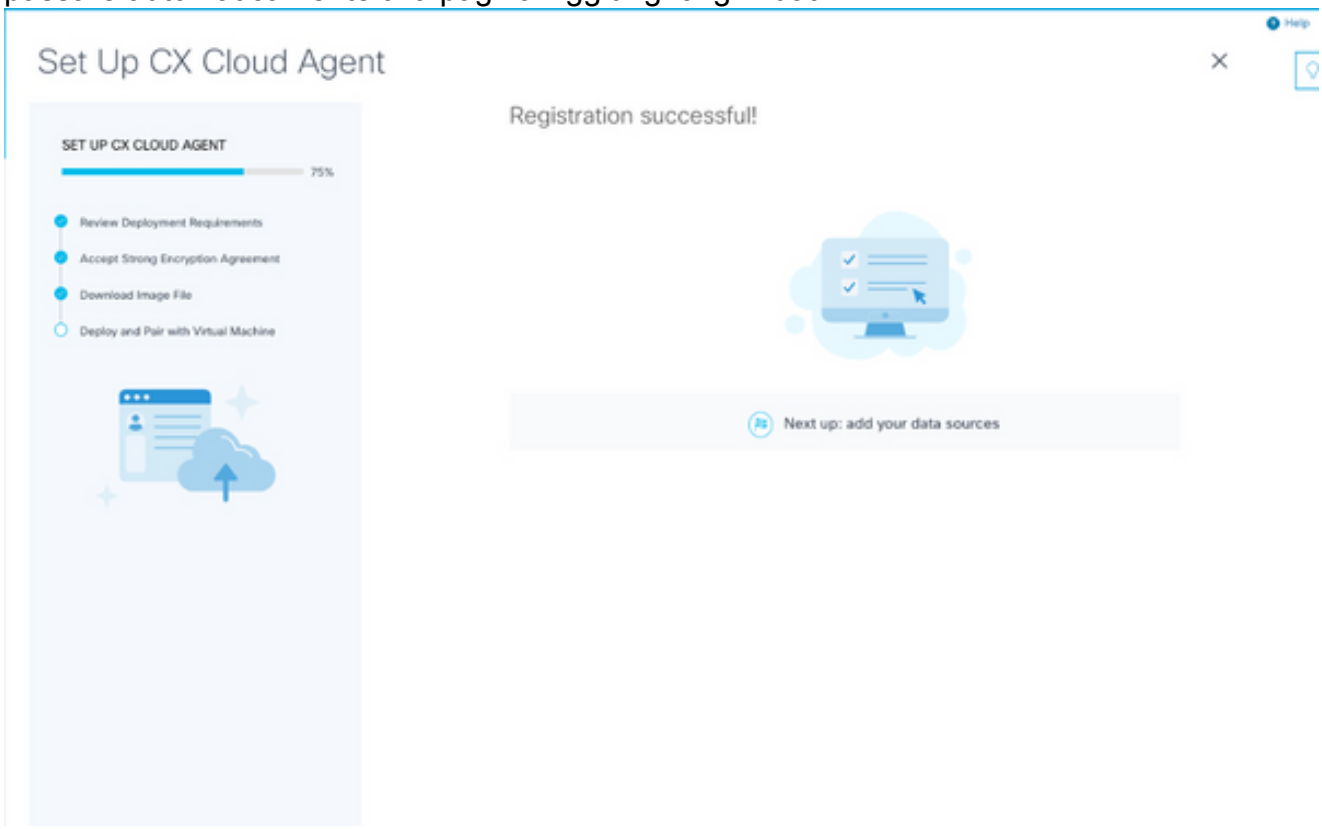
1. Immettere il codice di associazione fornito nella finestra di dialogo della console o nell'interfaccia della riga di comando (CLI) della macchina virtuale connessa tramite l'agente.

> Nota: il codice di associazione viene ricevuto dopo la distribuzione del file OVA scaricato.



Codice di associazione

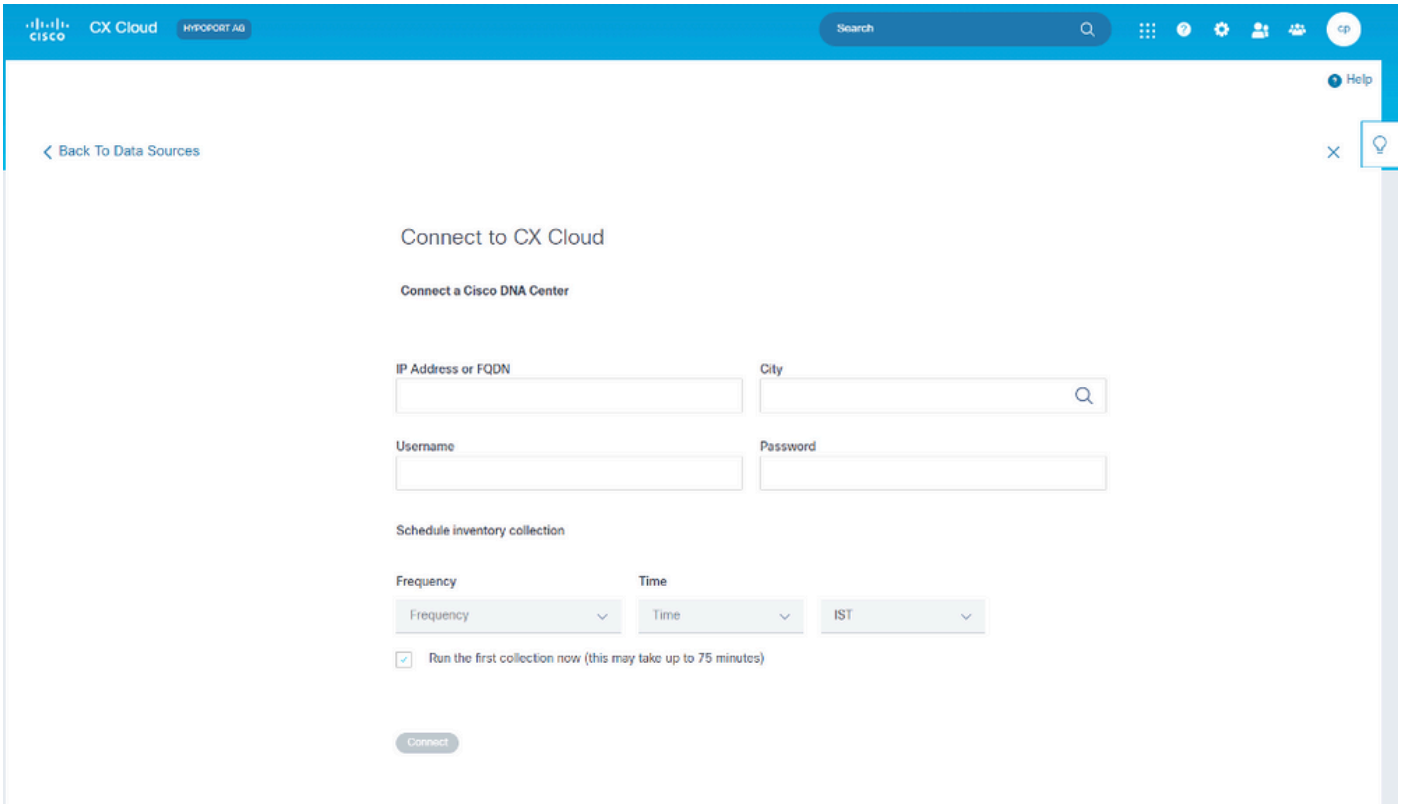
2. Fare clic su Continue (Continua) per registrare l'agente cloud CX. Viene visualizzata brevemente la finestra Impostazione agente cloud CX - Registrazione riuscita prima di passare automaticamente alla pagina Aggiungi origini dati.



Registrazione completata

Aggiunta di Cisco DNA Center come origine dati

Quando Cisco DNA Center viene selezionato dalla finestra di connessione delle origini dati (fare riferimento all'immagine Connect Data Sources nella sezione Connecting Data Sources), viene visualizzata la finestra seguente:



Connetti a CX Cloud

Per aggiungere Cisco DNA Center come origine dati:

1. Immettere l'indirizzo IP o l'indirizzo IP virtuale di Cisco DNA Center o l'FQDN, la città (ubicazione di Cisco DNA Center), il nome utente e la password.

   Nota: non utilizzare l'indirizzo IP di un singolo nodo cluster.

2. Pianificare una raccolta di inventario immettendo una Frequenza e un Tempo per indicare la frequenza con cui l'agente cloud CX può eseguire scansioni di rete e aggiornare le informazioni sui dispositivi collegati.

   Nota: la prima raccolta di magazzino può richiedere fino a 75 minuti.

3. Fare clic su Connetti. Viene visualizzata una conferma con l'indirizzo IP di Cisco DNA Center.

Connessione completata

4. Fare clic su Add Another Cisco DNA Center, Done o Back to Data Sources per tornare alla finestra Origini dati.

Aggiunta di altri cespiti come origini dati

Panoramica

La raccolta di dati di telemetria è stata estesa ai dispositivi non gestiti dal Cisco DNA Center, consentendo ai clienti di visualizzare e interagire con dati di analisi e informazioni derivati dalla telemetria per una gamma più ampia di dispositivi. Dopo la configurazione iniziale dell'agente cloud CX, gli utenti hanno la possibilità di configurare l'agente cloud CX per la connessione a 20 ulteriori Cisco DNA Center all'interno dell'infrastruttura monitorata da CX Cloud. Gli utenti possono inoltre connettere l'agente cloud CX direttamente ad altre risorse hardware del proprio ambiente, fino a 10.000 dispositivi collegati direttamente.

Gli utenti possono identificare i dispositivi da incorporare in CX Cloud identificando in modo univoco tali dispositivi utilizzando un file di inizializzazione o specificando un intervallo IP, che può essere analizzato dall'agente di CX Cloud. Entrambi gli approcci si basano sul protocollo SNMP (Simple Network Management Protocol) per il rilevamento (SNMP) e su SSH (Secure Shell) per la connettività. Questi devono essere configurati correttamente per abilitare la raccolta di telemetria.

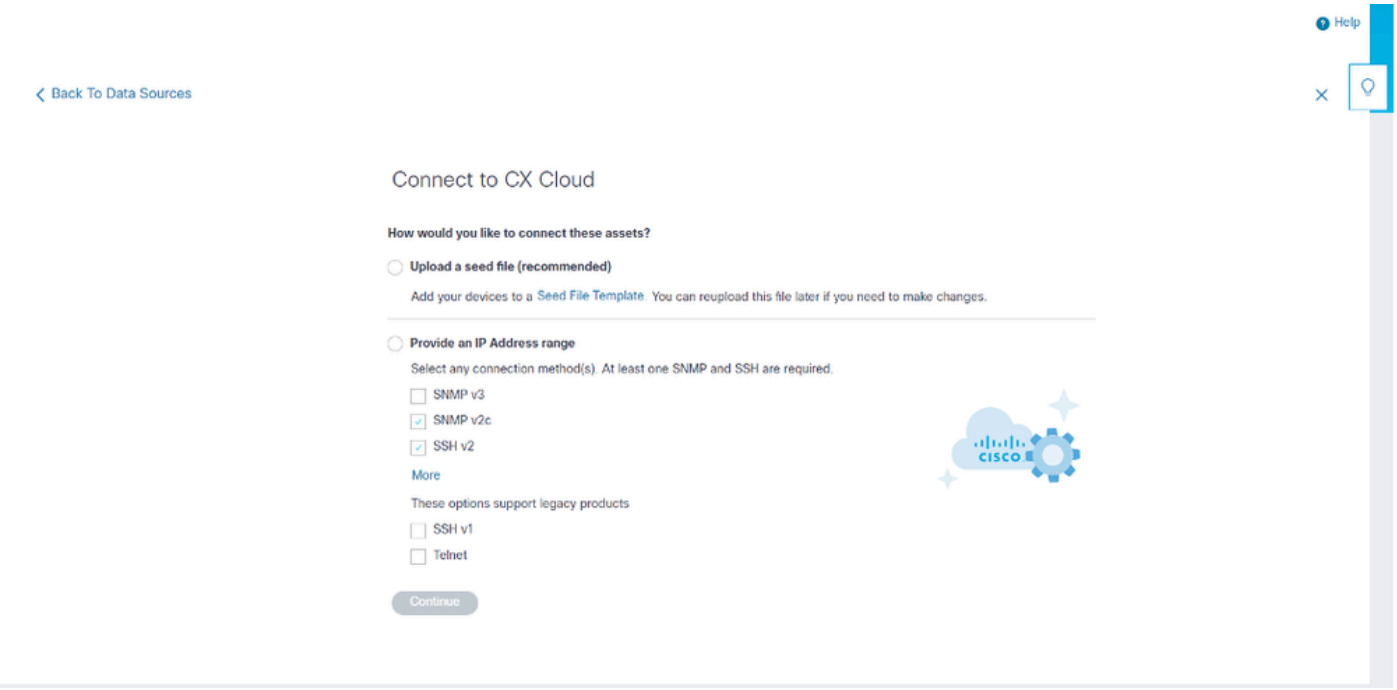
Nota:
È possibile utilizzare il file di origine o l'intervallo IP. Non è possibile modificare questa selezione dopo la configurazione iniziale.

Nota:
Un file di inizializzazione iniziale può essere sostituito con un altro file di inizializzazione,

---

mentre un intervallo IP iniziale può essere modificato in un nuovo intervallo IP.

Quando si seleziona Altre attività dalla finestra di connessione delle origini dati, viene visualizzata la finestra seguente:



Configura connessione a CX Cloud

Per aggiungere altri cespiti come origini dati:

- Caricare un file di origine utilizzando un modello di file di origine.
- Specificare un intervallo di indirizzi IP.

Protocolli di rilevamento

Sia il rilevamento diretto di dispositivi basato su file che il rilevamento basato su intervalli IP si basano sul protocollo SNMP come protocollo di rilevamento. Esistono diverse versioni di SNMP, ma l'agente cloud CX supporta SNMPV2c e SNMP V3 ed è possibile configurare una o entrambe le versioni. Le stesse informazioni, descritte più avanti in dettaglio, devono essere fornite dall'utente per completare la configurazione e abilitare la connettività tra il dispositivo gestito da SNMP e il gestore del servizio SNMP.

SNMPV2c e SNMPV3 differiscono in termini di sicurezza e modello di configurazione remota. SNMPV3 utilizza un sistema avanzato di protezione crittografica che supporta la crittografia SHA per autenticare i messaggi e garantirne la privacy. Si consiglia di utilizzare il protocollo SNMPv3 su tutte le reti pubbliche e connesse a Internet per proteggere il sistema da rischi e minacce alla sicurezza. Su CX Cloud, è preferibile configurare SNMPv3 e non SNMPv2c, ad eccezione dei dispositivi legacy meno recenti che non dispongono del supporto integrato per SNMPv3. Se entrambe le versioni di SNMP sono configurate dall'utente, l'agente cloud CX può, per impostazione predefinita, tentare di comunicare con ciascun dispositivo utilizzando SNMPv3 e tornare a SNMPv2c se la comunicazione non può essere negoziata correttamente.

Protocolli di connettività

Nell'ambito della configurazione della connettività diretta del dispositivo, gli utenti devono specificare i dettagli del protocollo di connettività del dispositivo: SSH (o, in alternativa, telnet). È possibile usare SSHv2, tranne nel caso di singoli asset legacy che non dispongono del supporto integrato appropriato. Tenere presente che il protocollo SSHv1 contiene vulnerabilità fondamentali. In assenza di ulteriore sicurezza, i dati di telemetria e le attività sottostanti possono essere compromessi a causa di queste vulnerabilità quando ci si affida a SSHv1. Anche Telnet non è sicuro. Le informazioni sulle credenziali (nomi utente e password) inviate tramite telnet non vengono crittografate e pertanto possono essere compromesse in assenza di ulteriore protezione.

Aggiungere dispositivi utilizzando un file di inizializzazione

Informazioni sul file di inizializzazione

Un file di origine è un file con valori delimitati da virgole (csv) in cui ogni riga rappresenta un record di dati di sistema. In un file di inizializzazione, ogni record del file di inizializzazione corrisponde a un dispositivo univoco dal quale la telemetria può essere raccolta dall'agente cloud CX. Tutti i messaggi di errore o di informazione relativi a ciascuna voce di dispositivo del file di origine da importare vengono acquisiti come parte dei dettagli del log del processo. Tutti i dispositivi in un file di inizializzazione sono considerati dispositivi gestiti, anche se non sono raggiungibili al momento della configurazione iniziale. Nel caso in cui venga caricato un nuovo file di origine per sostituire un file precedente, la data dell'ultimo caricamento viene visualizzata in CX Cloud.

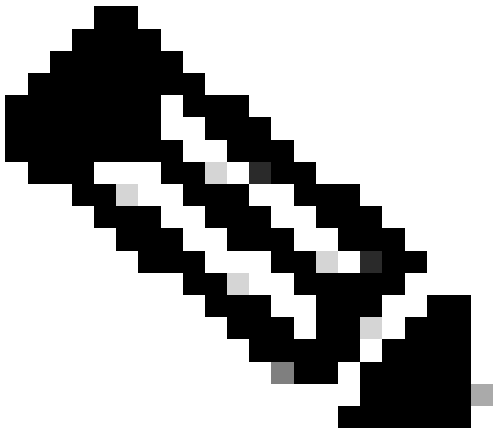
L'agente cloud CX può tentare di connettersi ai dispositivi, ma non può elaborarli singolarmente per visualizzarli nelle pagine Asset nei casi in cui non è in grado di determinare i PID o i numeri di serie. Qualsiasi riga nel file di origine che inizia con un punto e virgola viene ignorata. La riga di intestazione nel file di origine inizia con un punto e virgola e può essere mantenuta invariata (opzione consigliata) o eliminata durante la creazione del file di origine del cliente.

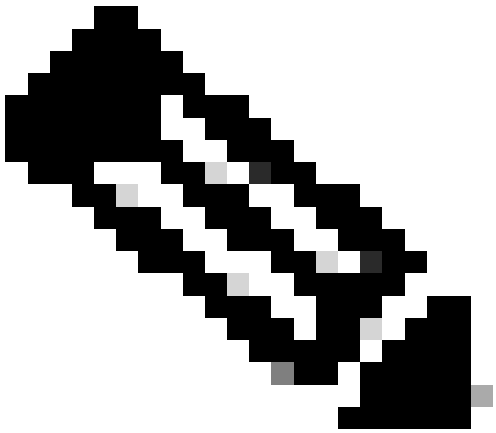
È importante che il formato del file di inizializzazione di esempio, incluse le intestazioni di colonna, non venga alterato in alcun modo. Fare clic sul collegamento fornito per visualizzare un file di origine in formato PDF. Questo PDF è solo a scopo di riferimento e può essere utilizzato per creare un file di origine che deve essere salvato in formato .csv.

Fare clic su questo collegamento per visualizzare un file di origine che può essere utilizzato per creare un file di origine in formato CSV.

Nota: questo PDF è solo a scopo di riferimento e può essere utilizzato per creare un file di origine che deve essere salvato in formato CSV.

Questa tabella identifica tutte le colonne necessarie del file di partenza e i dati da includere in ogni colonna.

Colonna file di inizializzazione	Intestazione/identificatore colonna	Scopo della colonna
A	Indirizzo IP o nome host	Specificare un indirizzo IP o un nome host valido e univoco per il dispositivo.
B	Versione protocollo SNMP	Il protocollo SNMP è richiesto dall'agente cloud CX e viene utilizzato per il rilevamento dei dispositivi all'interno della rete del cliente. I valori possono essere snmpv2c o snmpv3, ma per motivi di sicurezza è consigliabile utilizzare snmpv3.
C	snmpRo : obbligatorio se col#=3 è selezionato come 'snmpv2c'	Se la variante legacy di SNMPv2 è selezionata per un dispositivo specifico, è necessario specificare le credenziali snmpRO (sola lettura) per la raccolta SNMP del dispositivo. In caso contrario, l'immissione può essere vuota.
D	snmpv3UserName : obbligatorio se col#=3 è selezionato come 'snmpv3'	Se si seleziona SNMPv3 per comunicare con un dispositivo specifico, è necessario fornire il nome utente per l'accesso.
S	snmpv3AuthAlgorithm: i valori possono essere MD5 o SHA	Il protocollo SNMPv3 consente l'autenticazione tramite l'algoritmo MD5 o SHA. Se il dispositivo è configurato con l'autenticazione protetta, è necessario fornire il rispettivo algoritmo di autenticazione. 

Colonna file di inizializzazione	Intestazione/identificatore colonna	Scopo della colonna
		Nota: MD5 è considerato non sicuro e può essere utilizzato su tutti i dispositivi che lo supportano.
F	snmpv3AuthPassword: password	Se sul dispositivo è configurato un algoritmo di crittografia MD5 o SHA, è necessario fornire la password di autenticazione appropriata per l'accesso al dispositivo.
G	snmpv3PrivAlgorithm: i valori possono essere DES, 3DES	Se il dispositivo è configurato con l'algoritmo per la privacy SNMPv3 (questo algoritmo viene utilizzato per crittografare la risposta), è necessario fornire il rispettivo algoritmo.  Nota: le chiavi a 56 bit utilizzate da DES sono considerate troppo brevi per garantire la protezione crittografica e 3DES può essere utilizzato su tutti i dispositivi che lo supportano.
H	snmpv3PrivPassword: password	Se l'algoritmo per la privacy SNMPv3 è configurato sul dispositivo, è necessario fornire la rispettiva password per la privacy per la connessione al dispositivo.

Colonna file di inizializzazione	Intestazione/identificatore colonna	Scopo della colonna
I	snmpv3EngineId : engineID, ID univoco che rappresenta il dispositivo. Specificare l'ID del motore se configurato manualmente nel dispositivo	L'ID motore SNMPv3 è un ID univoco che rappresenta ciascun dispositivo. Questo ID motore viene inviato come riferimento durante la raccolta dei dataset SNMP da parte dell'agente cloud CX. Se il cliente configura il EngineID manualmente, è necessario fornire il relativo EngineID.
J	cliProtocol: i valori possono essere 'telnet', 'sshv1', 'sshv2'. Se vuoto, è possibile impostare 'sshv2' per impostazione predefinita	La CLI ha lo scopo di interagire direttamente con il dispositivo. CX Cloud Agent utilizza questo protocollo per la raccolta CLI per un dispositivo specifico. Questi dati di raccolta CLI vengono utilizzati per il reporting di asset e altre informazioni approfondite all'interno di CX Cloud. Si consiglia SSHv2; in assenza di altre misure di sicurezza della rete, i protocolli SSHv1 e Telnet non garantiscono un'adeguata sicurezza del trasporto.
K	cliPort : numero porta protocollo CLI	Se si seleziona un protocollo CLI, è necessario fornire il relativo numero di porta. Ad esempio, 22 per SSH e 23 per telnet.
L	cliUser : nome utente CLI (è possibile specificare nome utente/password CLI o ENTRAMBI, MA le colonne (col#=12 e col#=13) non possono essere vuote.)	È necessario fornire il nome utente CLI corrispondente del dispositivo. Viene utilizzato dall'agente cloud CX al momento della connessione al dispositivo durante la raccolta CLI.
M	cliPassword : password utente CLI (è possibile specificare nome utente/password CLI o BOTH, MA le colonne (col#=12 e col#=13) non possono essere vuote.)	È necessario fornire la password CLI corrispondente del dispositivo. Viene utilizzato dall'agente cloud CX al momento della connessione al dispositivo durante la raccolta CLI.
N	cliAttivaUtente	Se sul dispositivo è configurato enable, è

Colonna file di inizializzazione	Intestazione/identificatore colonna	Scopo della colonna
		necessario fornire il valore enableUsername del dispositivo.
O	cliAttivaPassword	Se sul dispositivo è configurato enable, è necessario fornire il valore enablePassword del dispositivo.
P	Supporto futuro (nessun input richiesto)	Riservato per un utilizzo futuro
Q	Supporto futuro (nessun input richiesto)	Riservato per un utilizzo futuro
R	Supporto futuro (nessun input richiesto)	Riservato per un utilizzo futuro
S	Supporto futuro (nessun input richiesto)	Riservato per un utilizzo futuro

Limitazioni all'elaborazione della telemetria per i dispositivi

Queste sono limitazioni nell'elaborazione dei dati di telemetria per i dispositivi:

- Alcuni dispositivi possono essere visualizzati come raggiungibili nel Riepilogo raccolta ma non sono visibili nella pagina Risorse del cloud CX. Le limitazioni della strumentazione del dispositivo impediscono l'elaborazione della telemetria del dispositivo.
- Gli attributi di telemetria possono essere imprecisi o mancanti nella pagina CX Cloud Assets per i dispositivi che non fanno parte di Campus Success Track.
- Se un dispositivo delle raccolte di file di origine o di intervalli IP fa anche parte dell'inventario di Cisco DNA Center, il dispositivo viene segnalato solo una volta per la voce di Cisco DNA Center. La voce relativa al file di inizializzazione/intervallo IP non viene raccolta o elaborata per evitare la duplicazione.

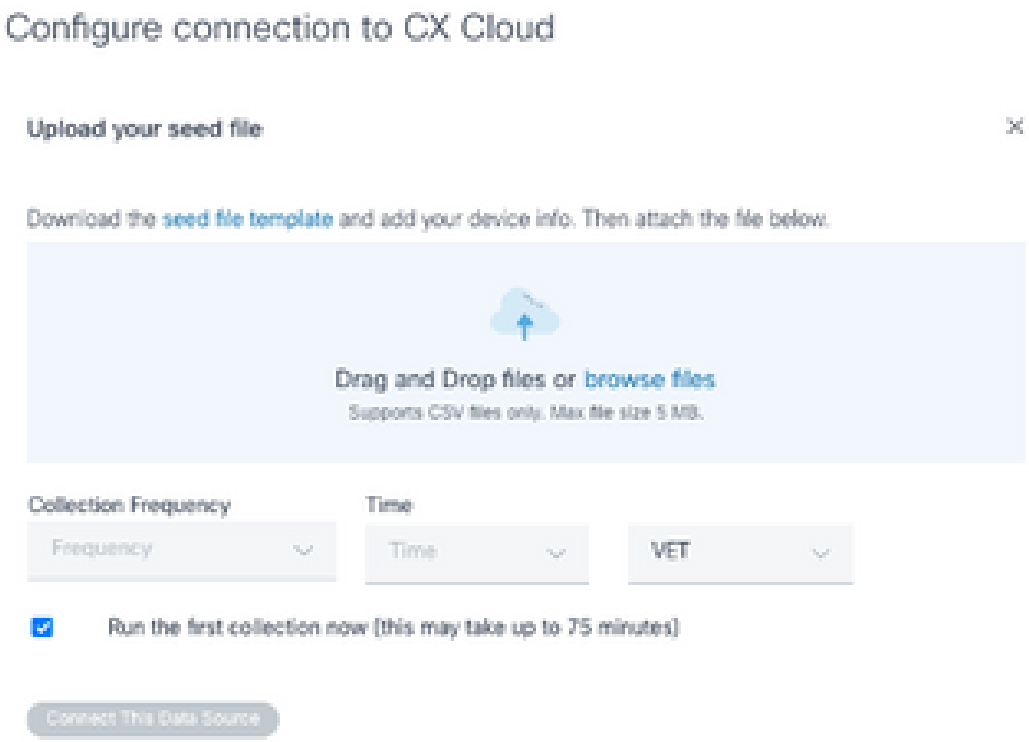
Aggiungi dispositivi utilizzando un nuovo file di inizializzazione

Per aggiungere dispositivi utilizzando un nuovo file di origine:

1. Scaricare il modello di file di inizializzazione (PDF) utilizzando il collegamento incorporato in

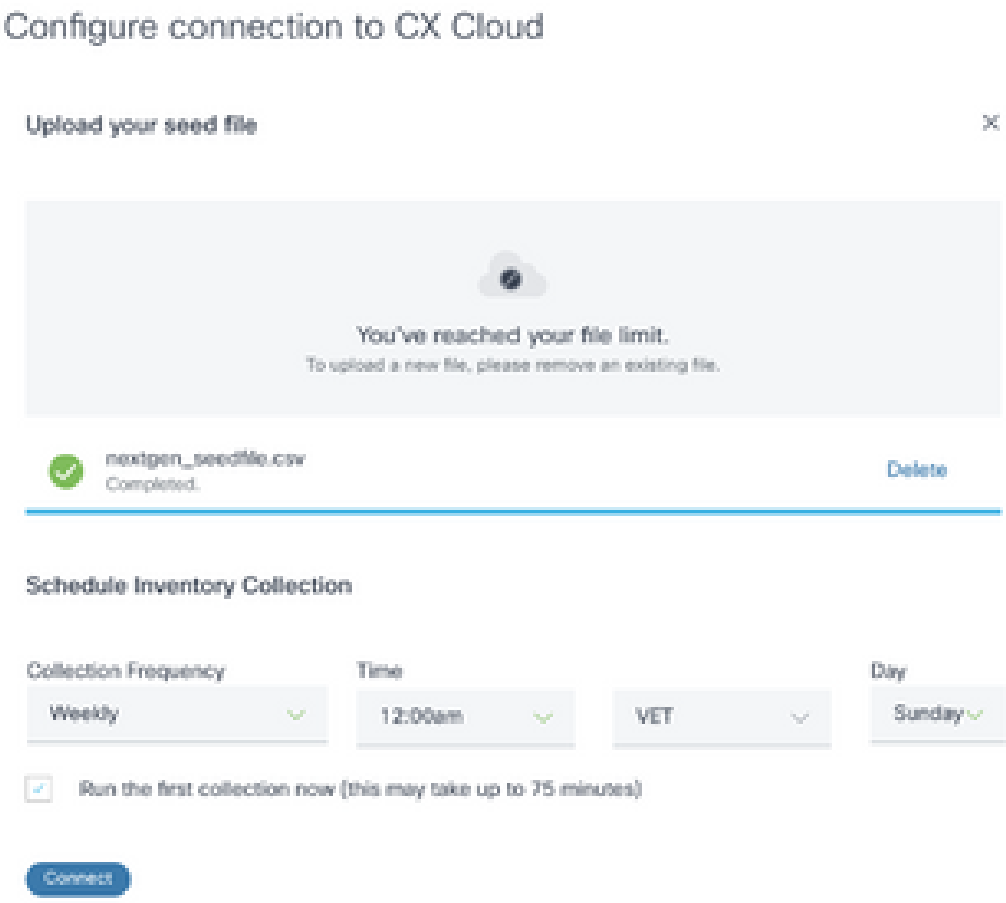
questo documento (fare riferimento a Informazioni sul file di inizializzazione) o tramite un collegamento nella finestra Configura connessione a CX Cloud.

Nota: il collegamento nella finestra Configura connessione a CX Cloud non è più disponibile dopo il download del file di inizializzazione iniziale.



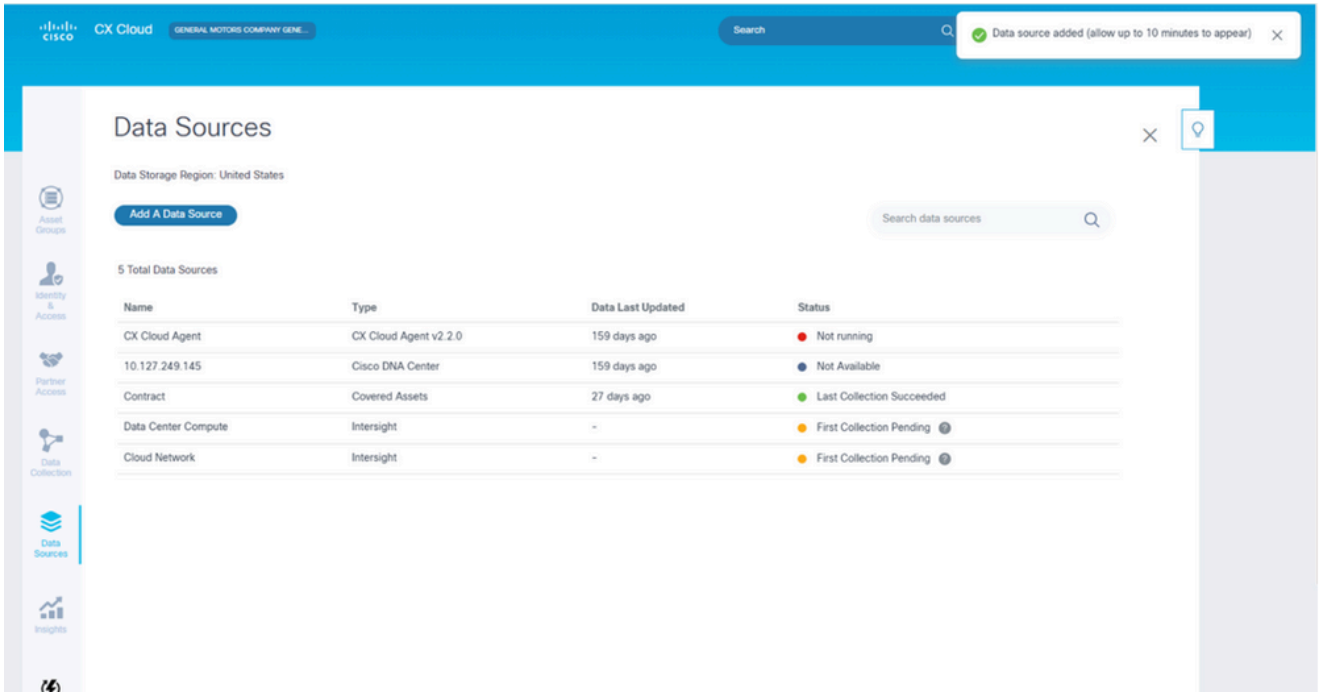
Finestra Configura connessione a CX Cloud

2. Aprire un foglio di calcolo di Excel (o un foglio di calcolo preferito) e immettere le intestazioni come illustrato nel modello.
3. Immettere i dati manualmente o importarli nel file.
4. Al termine, salvare il modello come file .csv per importare il file in CX Cloud Agent.



Finestra Carica file di inizializzazione

5. Nella finestra Upload your seed, trascinare e rilasciare il file .csv appena creato oppure fare clic su Browse files e individuare il file .csv.
6. Completare la sezione Pianifica raccolta scorte e fare clic su Connetti. Verrà visualizzata la finestra Origini dati contenente un messaggio di conferma.
7. Prima che la configurazione iniziale di CX Cloud sia completata, l'agente di CX Cloud deve eseguire la prima raccolta di telemetria elaborando il file di inizializzazione e stabilendo la connessione con tutti i dispositivi identificati. La raccolta può essere avviata su richiesta o eseguita in base a una pianificazione definita qui. Gli utenti possono eseguire la prima connessione di telemetria selezionando la casella di controllo Esegui la prima raccolta adesso. A seconda del numero di voci specificate nel file di inizializzazione e di altri fattori, questo processo può richiedere molto tempo.



Messaggio di conferma

Aggiungere dispositivi utilizzando un file di inizializzazione modificato

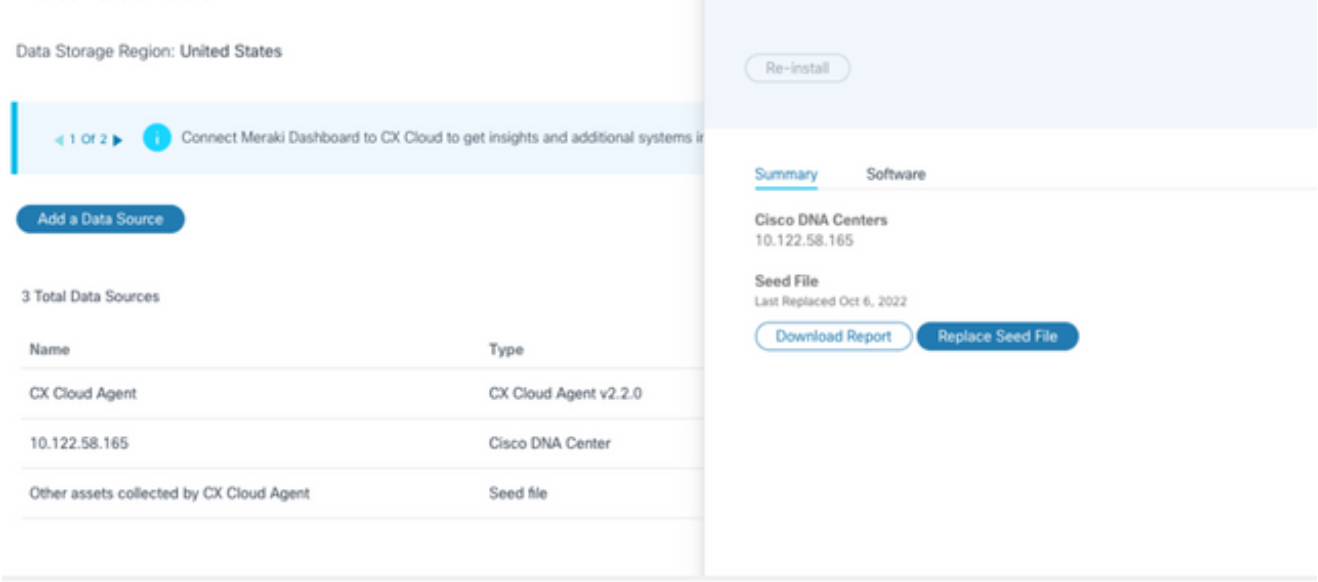
Per aggiungere, modificare o eliminare dispositivi utilizzando il file di origine corrente:

1. Aprite il file di origine creato in precedenza, apportate le modifiche necessarie e salvate il file.

Nota: per aggiungere cespiti al file di origine, aggiungete tali cespiti al file di origine creato in precedenza e ricaricate il file. Questa operazione è necessaria in quanto il caricamento di un nuovo file di inizializzazione sostituisce il file di inizializzazione corrente. Per l'individuazione e la raccolta viene utilizzato solo l'ultimo file di inizializzazione caricato.

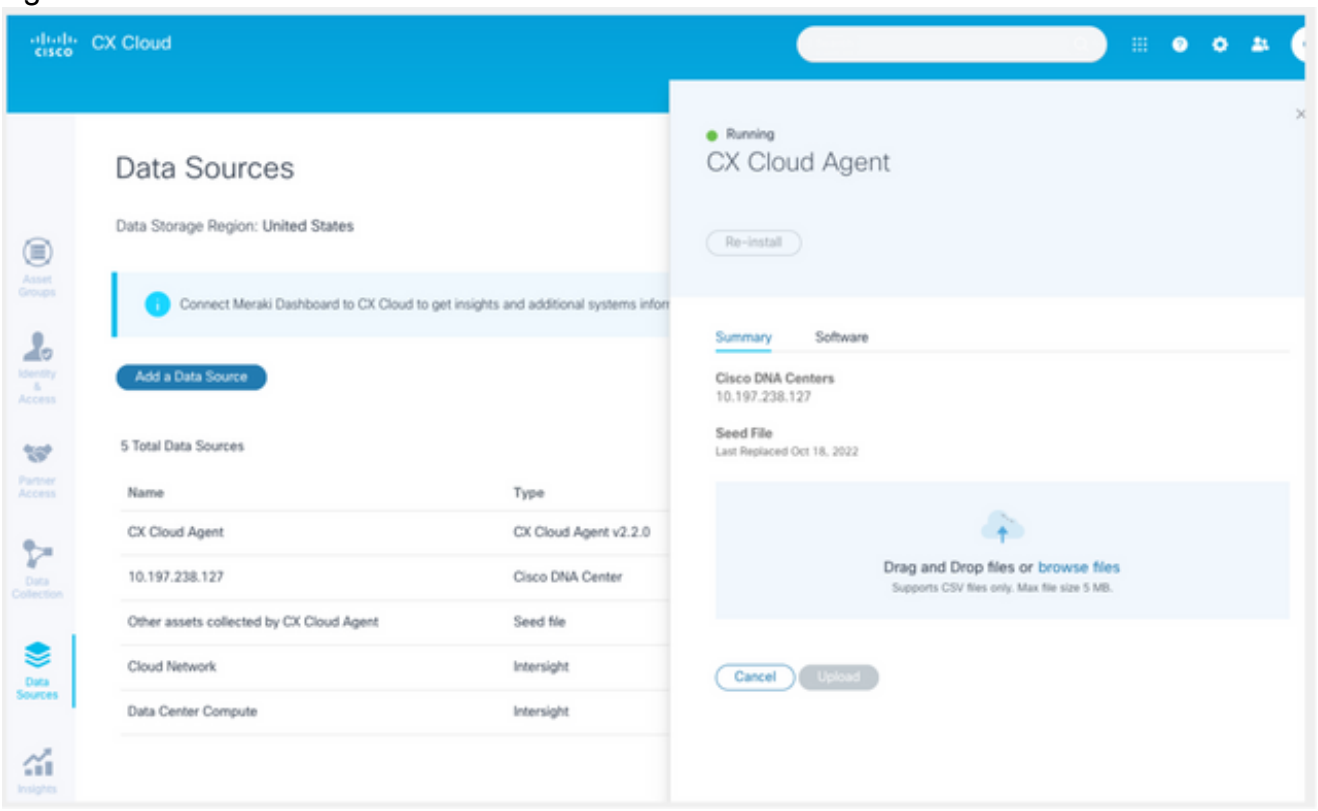
---

2. Dalla pagina Origini dati, selezionare un'origine dati che abbia un tipo di agente cloud CX. Viene visualizzata una finestra dei dettagli con le schede Riepilogo e Software.



Finestra Dettagli

3. Fare clic su Scarica report per generare un report su tutte le risorse per l'origine dati selezionata. Il report fornisce informazioni sull'indirizzo IP del dispositivo, il numero di serie, la raggiungibilità, il tipo di comando, lo stato del comando e l'errore del comando, se applicabile.
4. Fare clic su Sostituisci file di inizializzazione. Viene visualizzata la finestra di CX Cloud Agent.



Finestra di CX Cloud Agent

5. Trascinare e rilasciare il file di origine modificato nella finestra oppure selezionare il file e aggiungerlo nella finestra.
6. Fare clic su Upload.

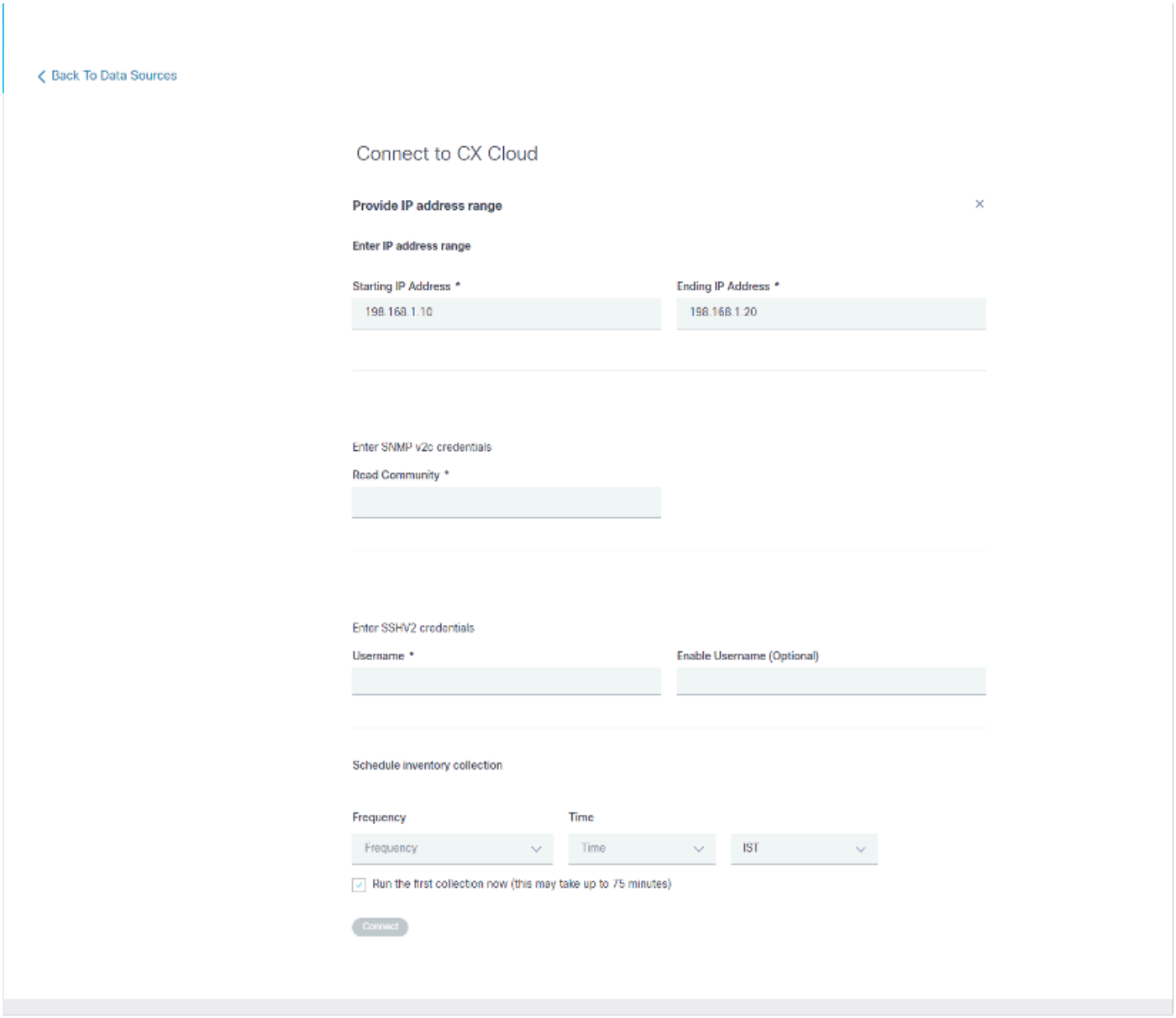
Aggiungi dispositivi tramite intervalli IP

Gli intervalli IP consentono agli utenti di identificare le risorse hardware e, di conseguenza, di raccogliere la telemetria da tali dispositivi in base agli indirizzi IP. I dispositivi per la raccolta di telemetria possono essere identificati in modo univoco specificando un singolo intervallo IP a livello di rete, che può essere analizzato dall'agente cloud CX utilizzando il protocollo SNMP. Se l'intervallo IP viene scelto per identificare un dispositivo connesso direttamente, gli indirizzi IP a cui si fa riferimento possono essere il più restrittivi possibile, consentendo al tempo stesso la copertura per tutti gli asset necessari.

- È possibile specificare indirizzi IP specifici oppure utilizzare caratteri jolly per sostituire gli ottetti di un indirizzo IP e creare un intervallo.
- Se uno specifico indirizzo IP non è incluso nell'intervallo IP identificato durante l'installazione, l'agente cloud CX non tenta di comunicare con un dispositivo che dispone di tale indirizzo IP, né raccoglie dati di telemetria da tale dispositivo.
- L'immissione di *.*.*.* consente all'agente cloud CX di utilizzare le credenziali fornite dall'utente con qualsiasi IP. Ad esempio: 172.16.*.* consente di utilizzare le credenziali per tutti i dispositivi della subnet 172.16.0.0/16.
- In caso di modifiche alla rete o alla base installata, è possibile modificare l'intervallo IP. Fare riferimento alla sezione Modifica degli intervalli IP

L'agente cloud CX può tentare di connettersi ai dispositivi ma non è in grado di elaborarli singolarmente per visualizzarli nella visualizzazione Asset nei casi in cui non è in grado di determinare i PID o i numeri di serie.

Note:
Facendo clic su Modifica intervallo indirizzi IP viene avviato il rilevamento dei dispositivi su richiesta. Quando un nuovo dispositivo viene aggiunto o eliminato (all'interno o all'esterno) a un intervallo IP specificato, il cliente deve sempre fare clic su Modifica intervallo indirizzi IP (fare riferimento alla sezione Modifica degli intervalli IP) e completare i passaggi richiesti per avviare il rilevamento dei dispositivi su richiesta per includere qualsiasi dispositivo appena aggiunto all'inventario della raccolta dell'agente cloud CX.



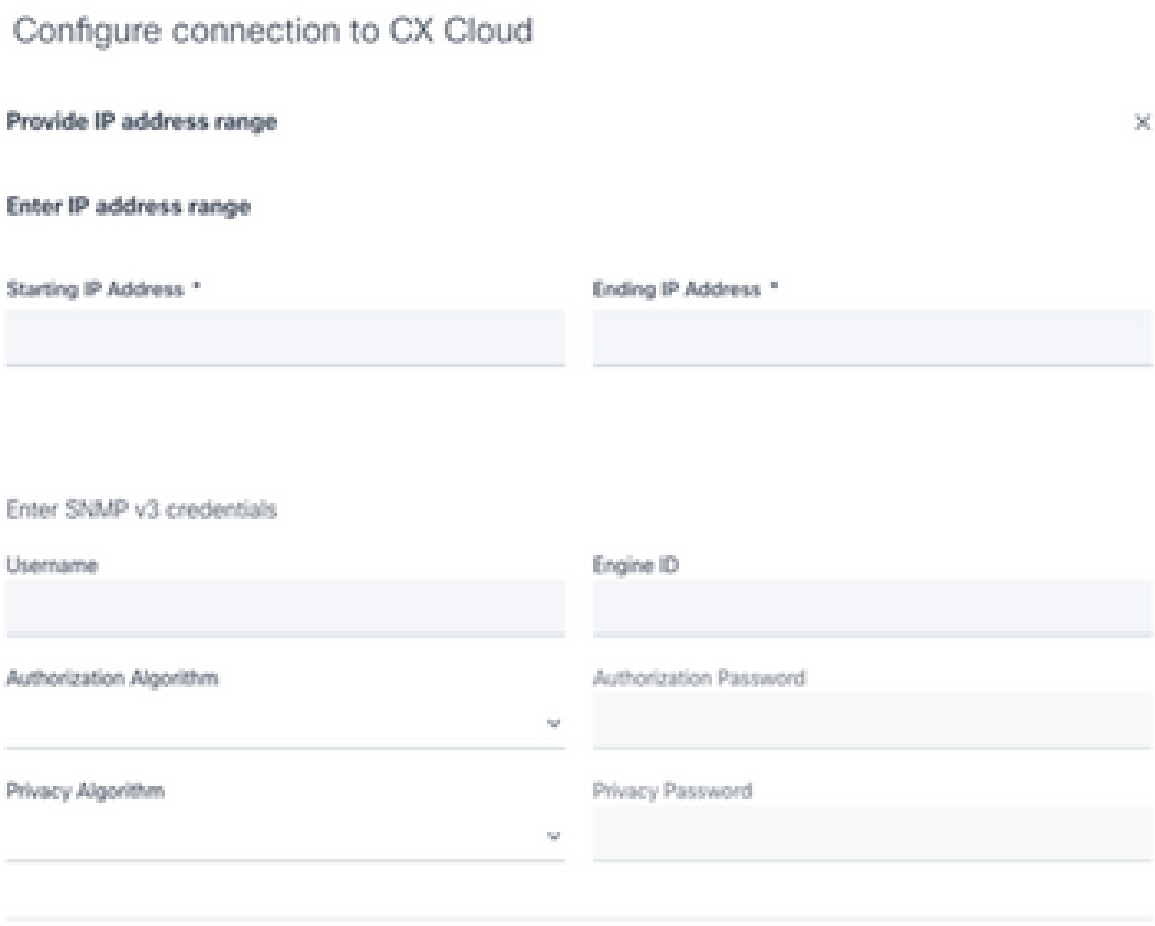
Finestra Intervallo di indirizzi IP iniziale

L'aggiunta di dispositivi tramite un intervallo IP richiede che gli utenti specifichino tutte le credenziali applicabili tramite l'interfaccia utente di configurazione. I campi visibili variano a seconda dei protocolli selezionati nelle finestre precedenti. Se si selezionano più protocolli per lo stesso protocollo, ad esempio SNMPv2c e SNMPv3 o SSHv2 e SSHv1, l'agente cloud CX negozia automaticamente la selezione del protocollo in base alle funzionalità del singolo dispositivo.

Quando si connettono dispositivi utilizzando indirizzi IP, il cliente può verificare che tutti i protocolli pertinenti nell'intervallo IP, insieme alle versioni SSH e alle credenziali Telnet, siano validi o che le connessioni non riescano.

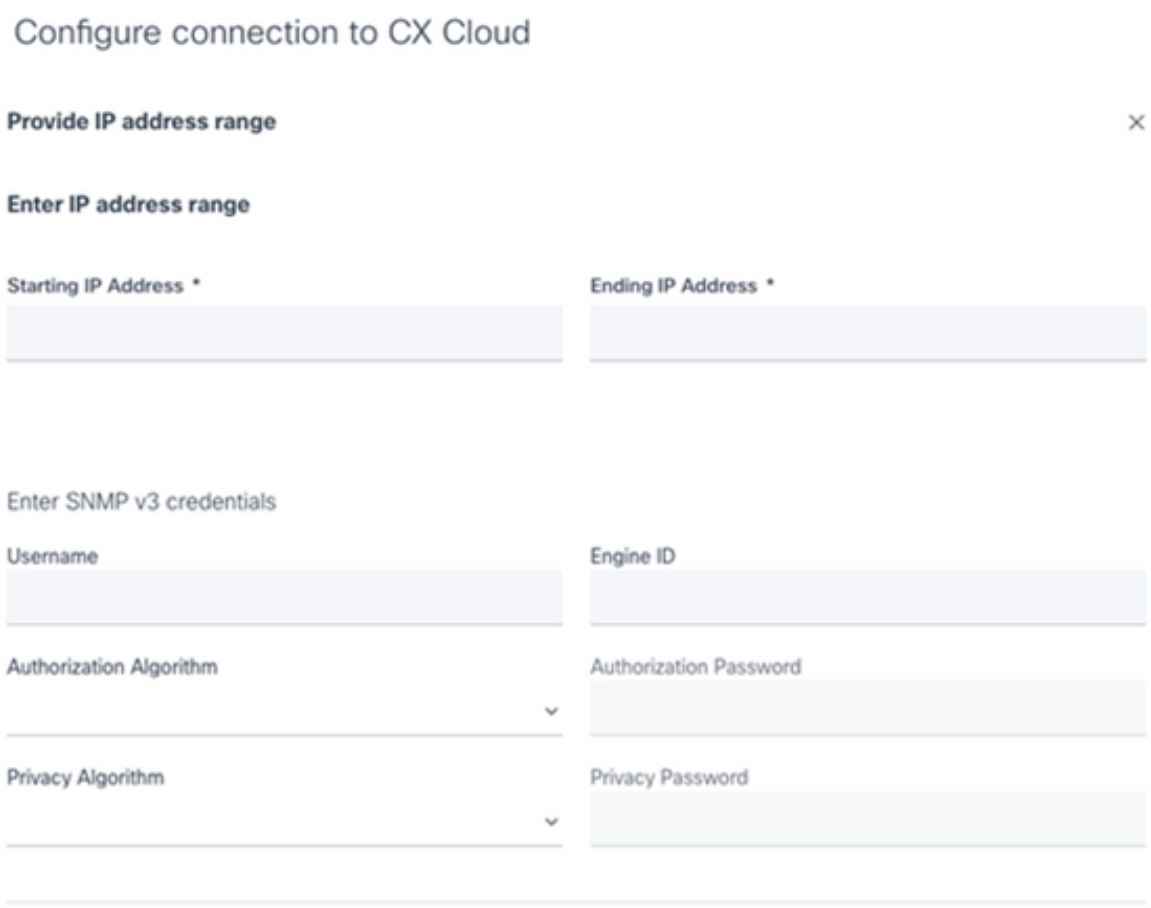
Per aggiungere dispositivi utilizzando l'intervallo IP:

1. Nella finestra Configure connection to CX Cloud, selezionare l'opzione Provide an IP Address range.

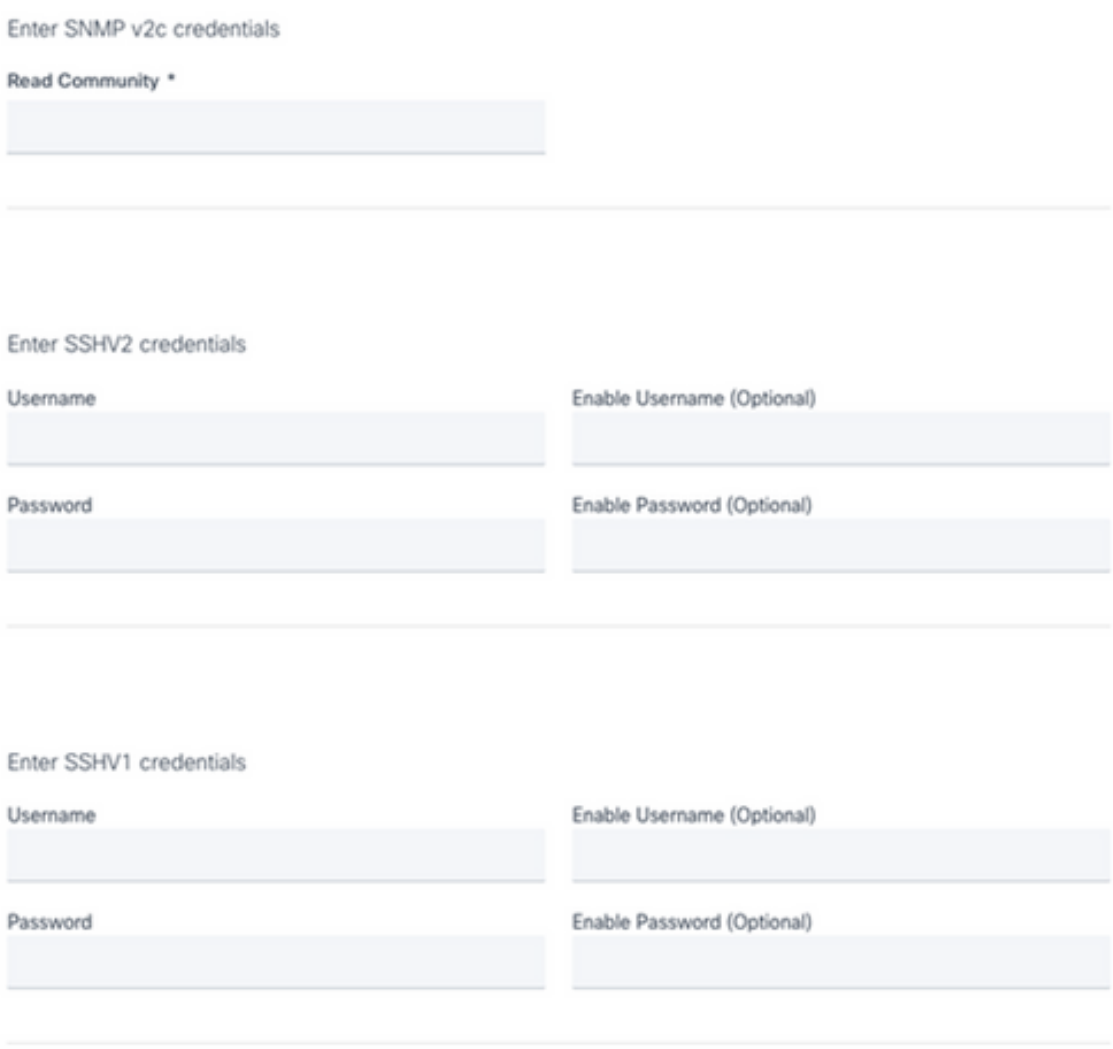


Modulo Aggiungi dispositivi tramite indirizzi IP

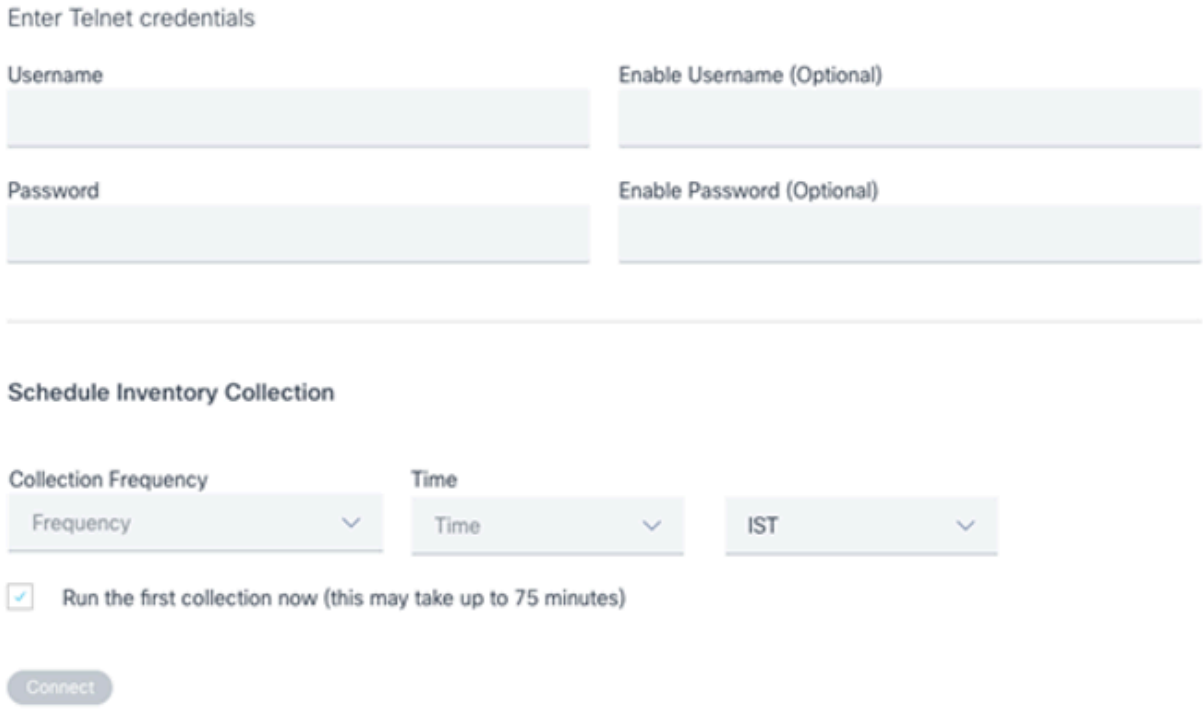
2. Completare il modulo con le informazioni pertinenti.
3. È possibile selezionare diverse opzioni di connessione. In queste schermate vengono visualizzate le credenziali di configurazione per le opzioni. Fare riferimento a Informazioni sul file di inizializzazione per una descrizione dei campi delle credenziali per ciascuna opzione di connessione.



Credenziali SNMP v3

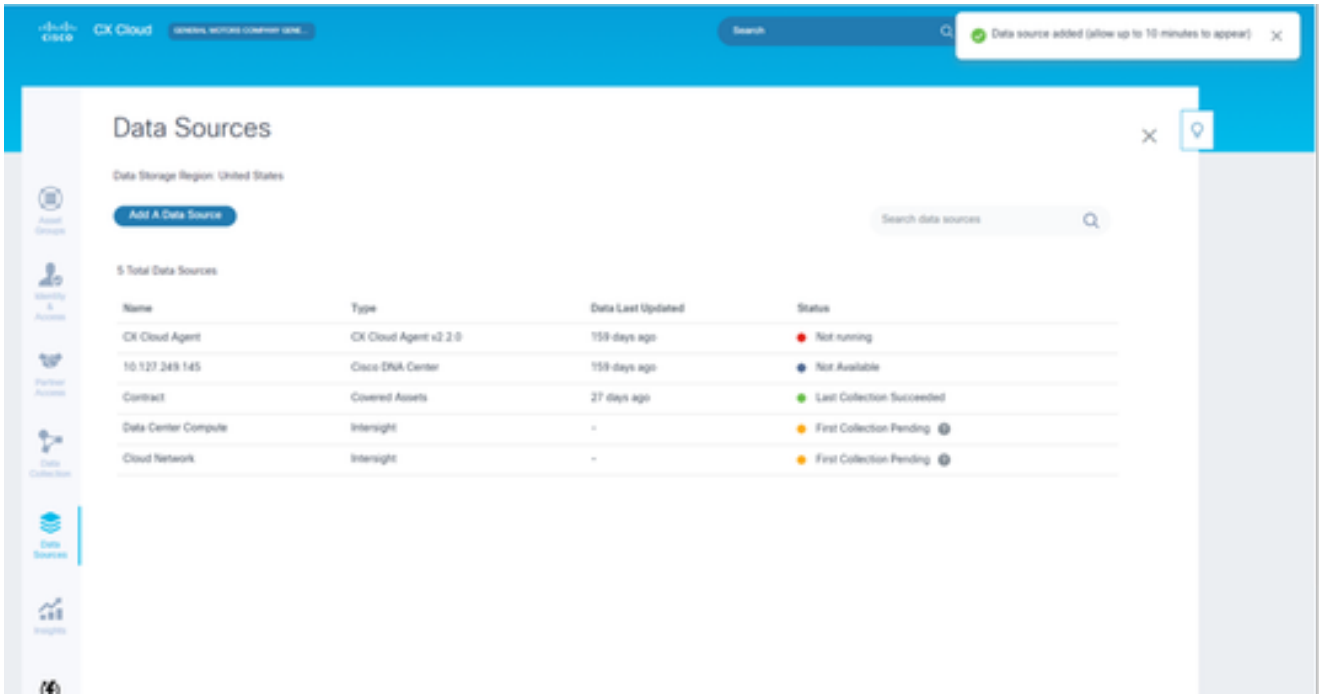


Credenziali SNMP v2, SSHV2 e SSHV1



Pianificazione delle credenziali Telnet e dell'analisi della rete

4. Fare clic su Connetti. Verrà visualizzata la finestra Origini dati contenente un messaggio di conferma.

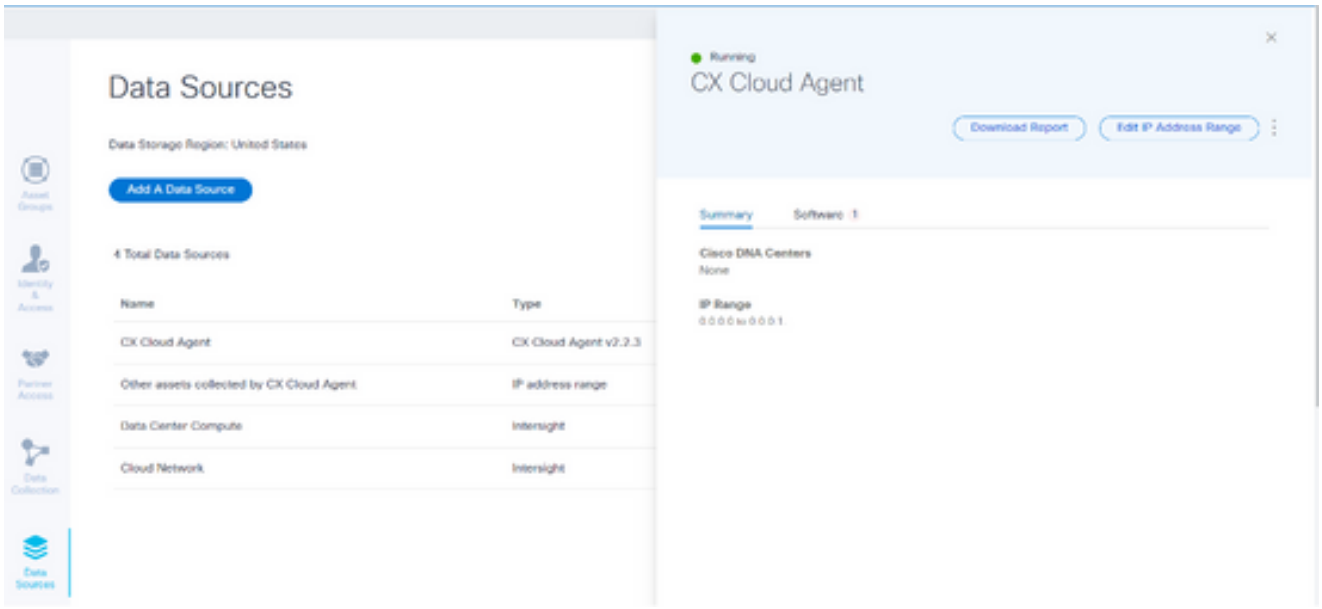


Conferma

Modifica degli intervalli IP

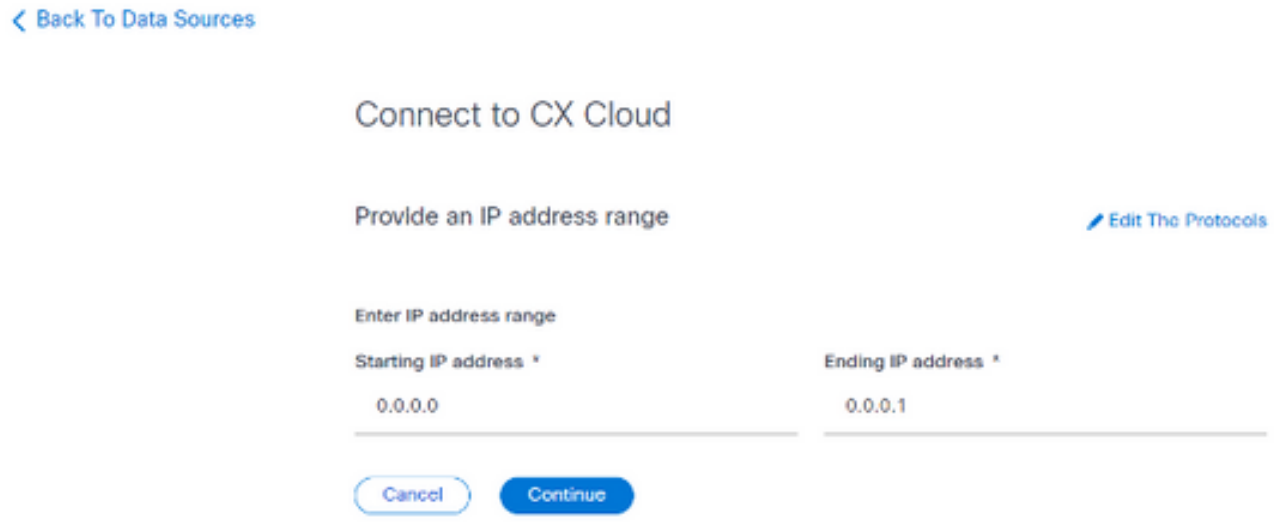
Per modificare un intervallo IP:

1. Passare alla finestra Origini dati.



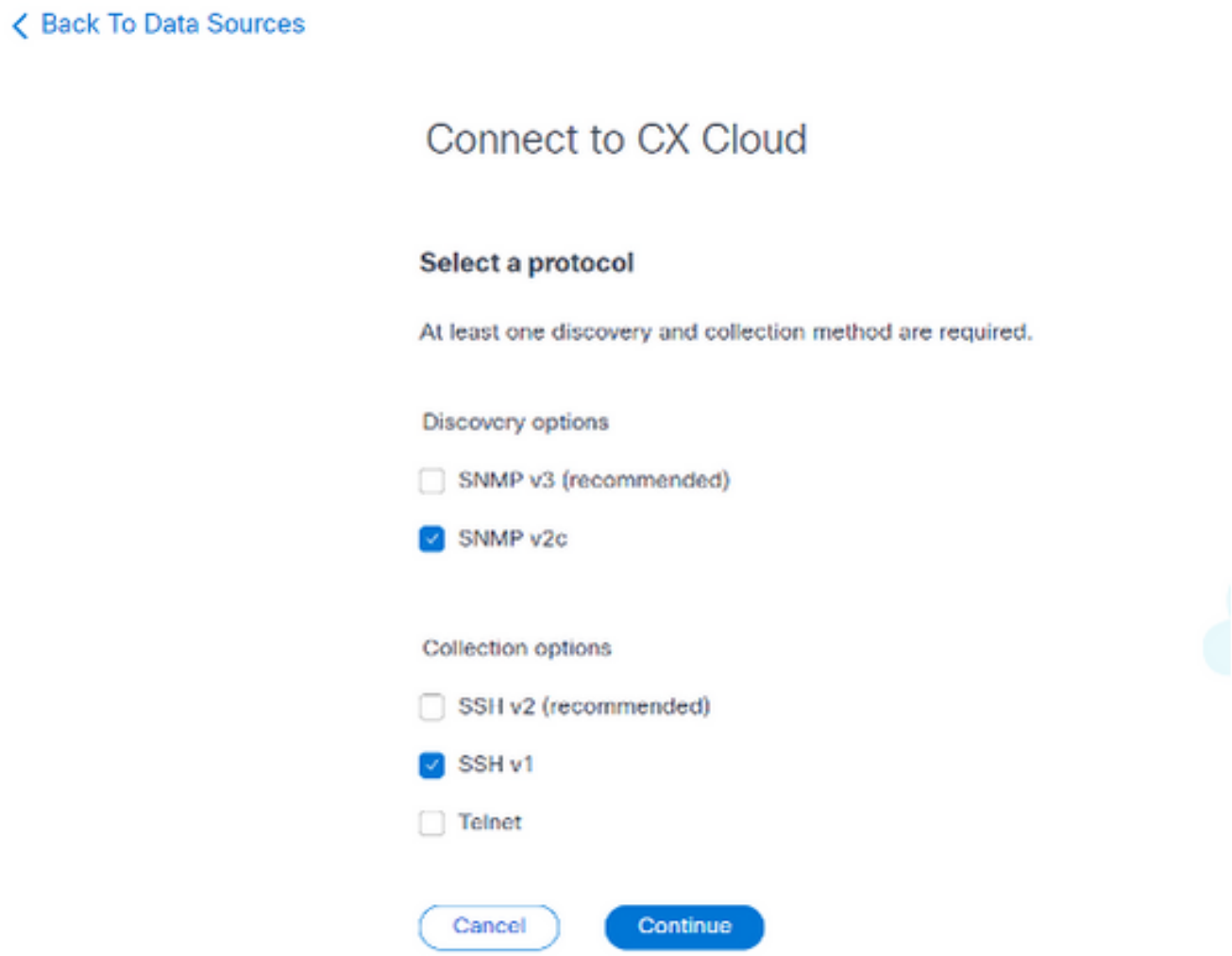
Origini dei dati

2. Fare clic sull'agente cloud CX che richiede la modifica dell'intervallo IP nelle origini dati. Viene visualizzata la finestra dei dettagli.
3. Fare clic su Modifica intervallo di indirizzi IP. Viene visualizzata la finestra Connetti a CX Cloud.



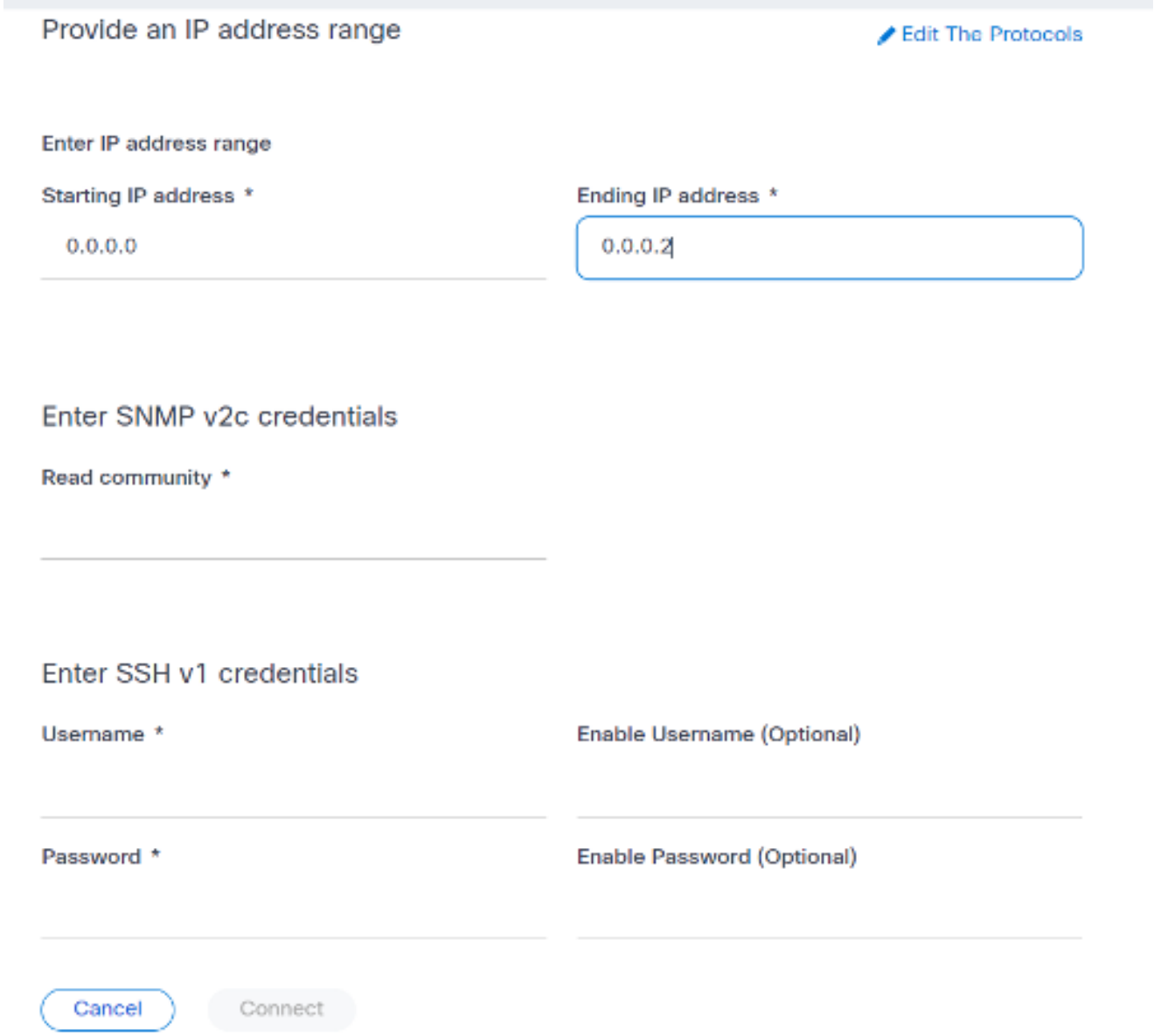
Fornire un intervallo IP

4. Aggiornare i nuovi indirizzi IP nei campi Indirizzo IP iniziale e Indirizzo IP finale.
5. Fare clic sul collegamento Modifica protocolli. Viene visualizzata la finestra Connect to CX Cloud - Select a protocol.



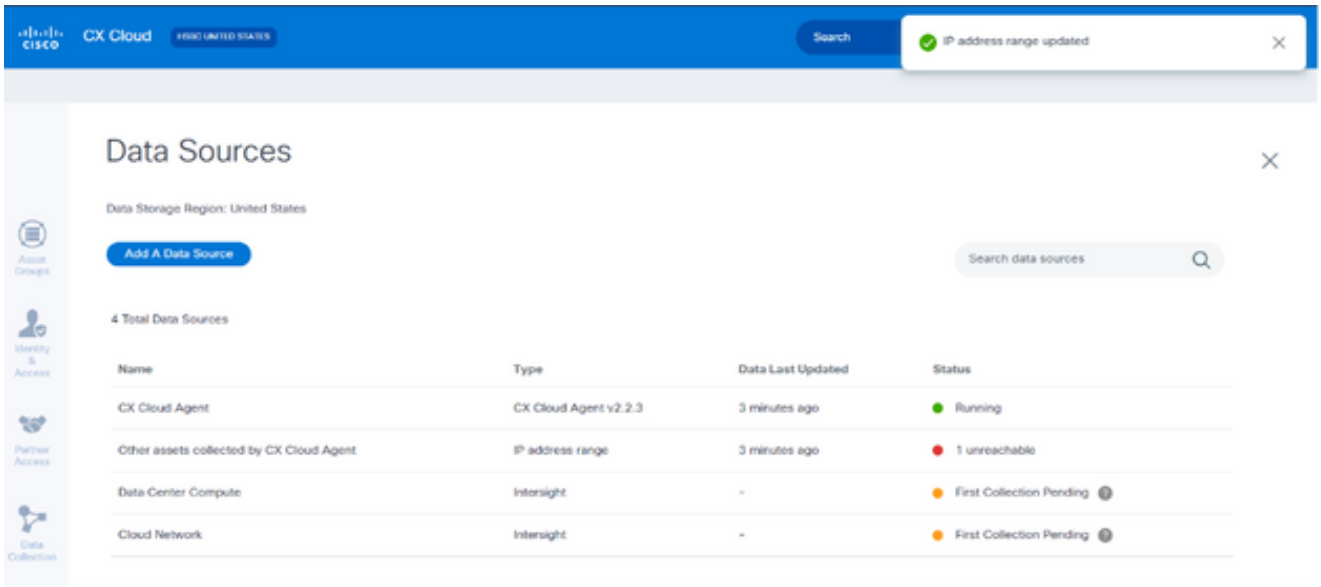
Seleziona protocollo

6. Selezionare i protocolli applicabili facendo clic sulle caselle di controllo appropriate.
7. Fare clic su Continue (Continua). Viene visualizzata la finestra Specifica intervallo di indirizzi IP.



Immetti credenziali

8. Immettere le credenziali di configurazione.
9. Fare clic su Connetti. Verrà visualizzata la finestra Origini dati contenente un messaggio di conferma.



Conferma

Nota: il messaggio di conferma non garantisce che i dispositivi nell'intervallo modificato siano raggiungibili e che le credenziali siano state accettate.

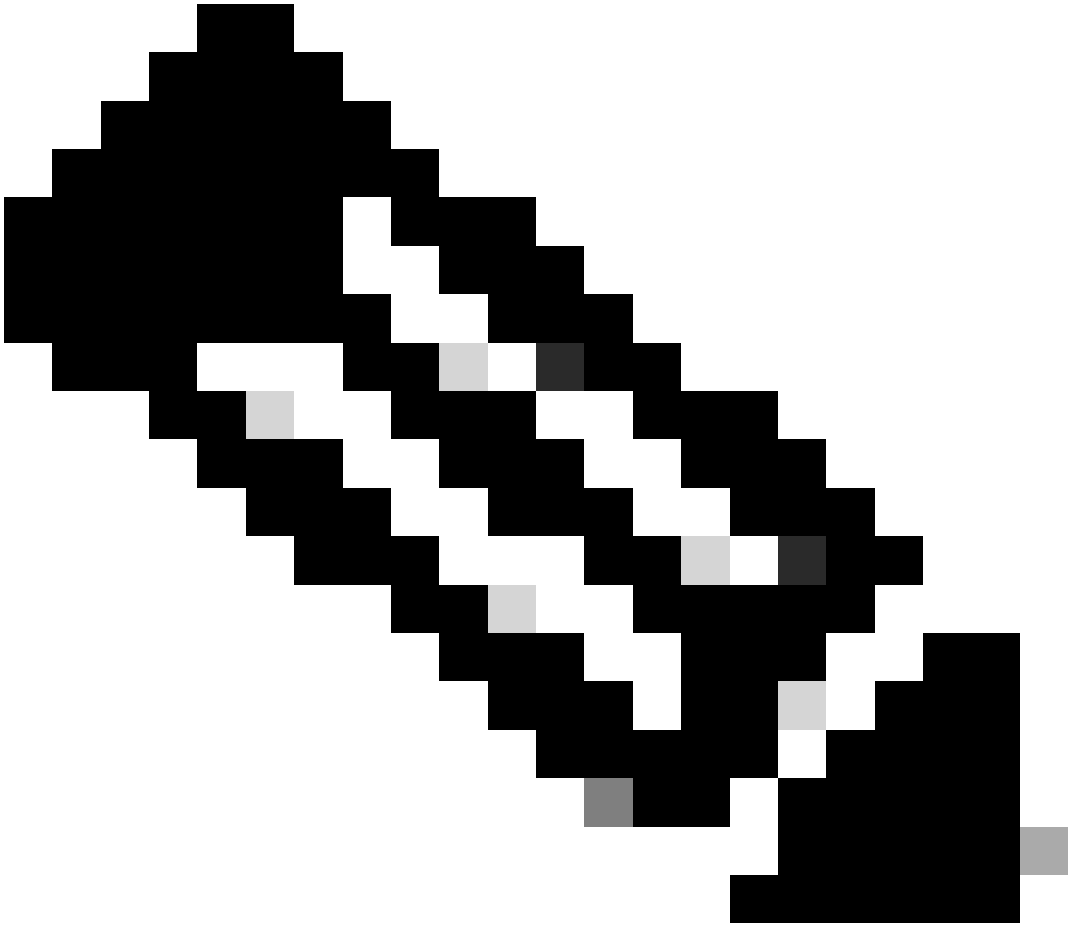
Informazioni sui dispositivi rilevati da più controller

È possibile che alcuni dispositivi possano essere individuati sia da Cisco DNA Center che dalla connessione diretta dei dispositivi all'agente cloud CX, causando la raccolta di dati duplicati da tali dispositivi. Per evitare la raccolta di dati duplicati e la gestione dei dispositivi da parte di un solo controller, è necessario determinare una precedenza per la gestione dei dispositivi da parte dell'agente cloud CX.

- Se un dispositivo viene individuato per la prima volta da Cisco DNA Center e quindi riscoperto tramite connessione diretta (utilizzando un file di inizializzazione o un intervallo IP), Cisco DNA Center ha la precedenza nel controllo del dispositivo.
- Se un dispositivo viene individuato per la prima volta tramite connessione diretta al dispositivo all'agente cloud CX e quindi riscoperto da Cisco DNA Center, Cisco DNA Center ha la precedenza nel controllo del dispositivo.

Pianificazione delle analisi diagnostiche

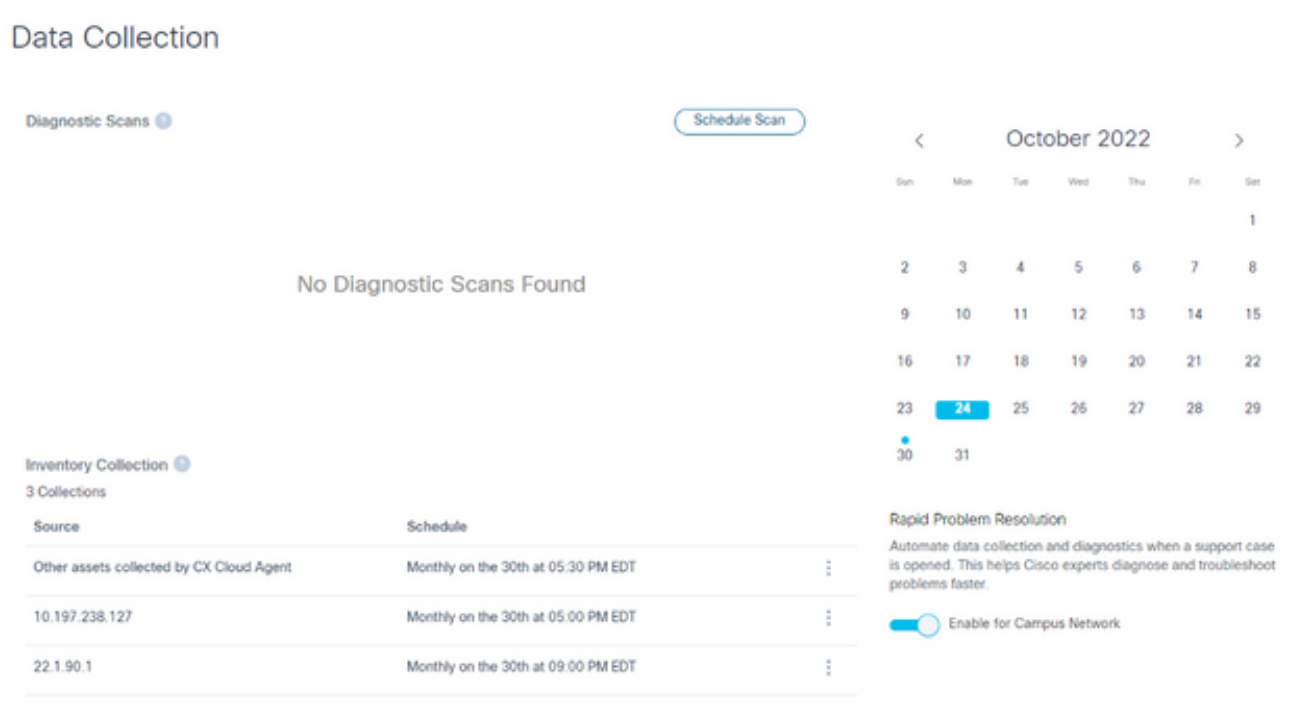
I clienti possono pianificare scansioni diagnostiche su richiesta in CX Cloud.



Nota: Cisco consiglia di pianificare le analisi diagnostiche o di avviare le analisi su richiesta almeno 6-7 ore prima dei programmi di raccolta delle scorte in modo che non si sovrappongano. L'esecuzione simultanea di più scansioni diagnostiche può rallentare il processo di scansione e potenzialmente causare errori di scansione.

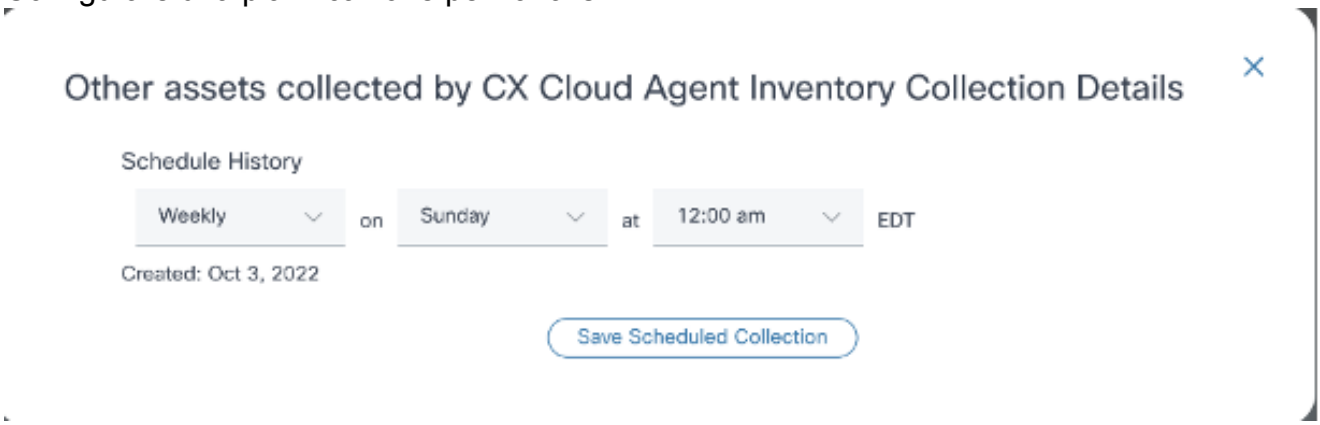
Per pianificare le analisi diagnostiche:

1. Nella pagina Home fare clic sull'icona Impostazioni (ingranaggio).
2. Nella pagina Origini dati selezionare Raccolta dati nel riquadro sinistro.
3. Fare clic su Pianifica scansione.



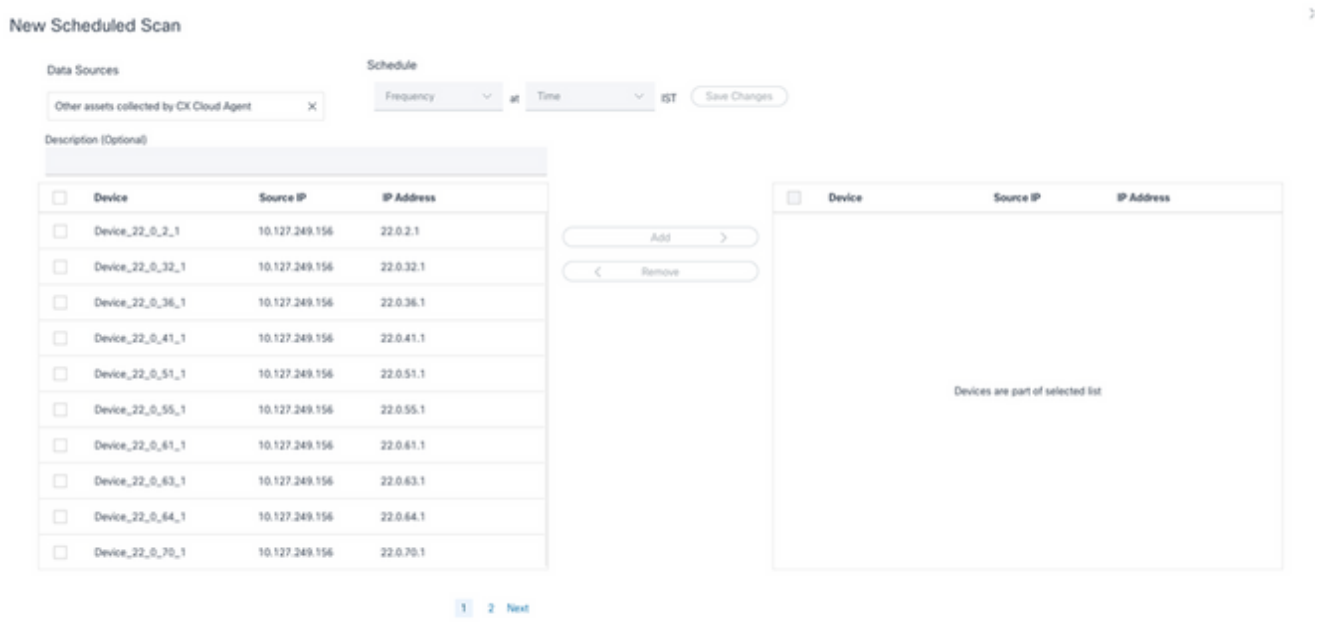
Raccolta dati

4. Configurare una pianificazione per l'analisi.



Configura pianificazione analisi

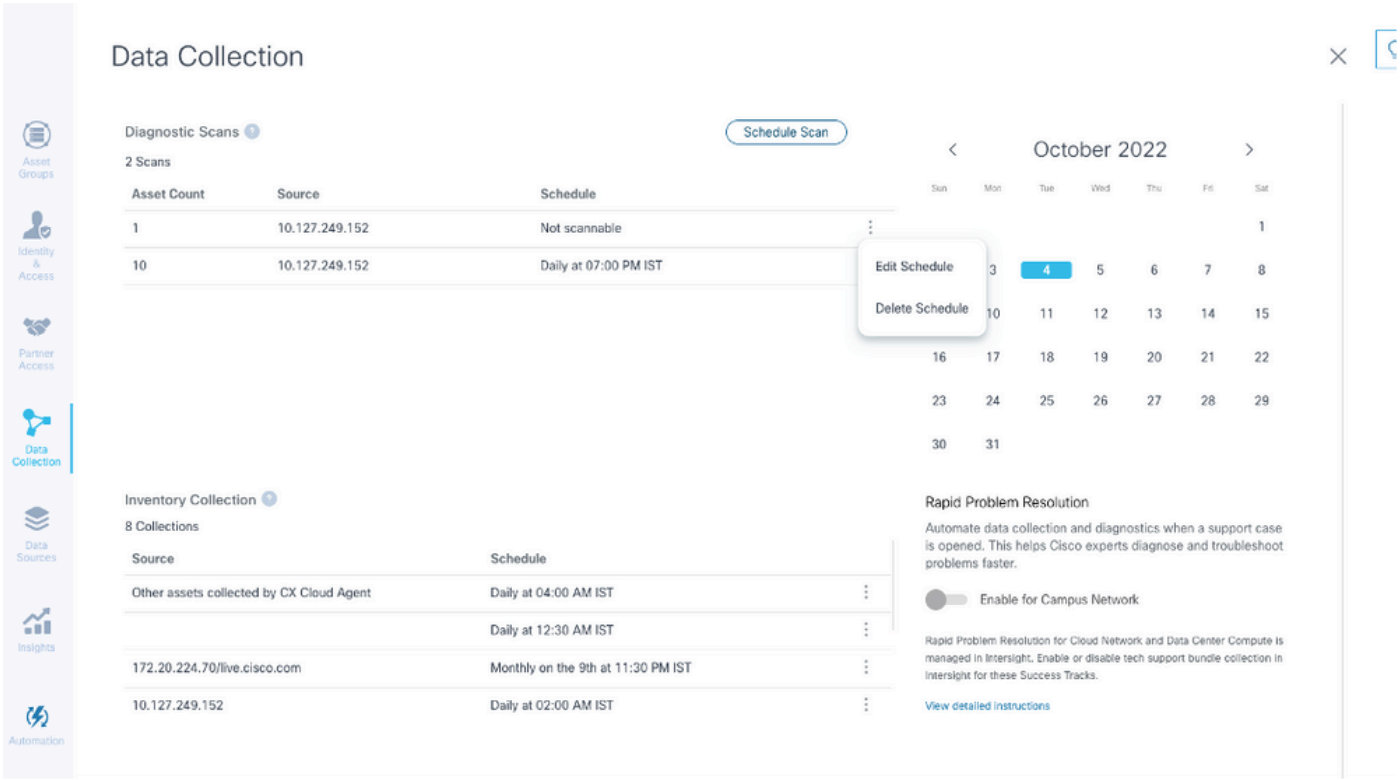
5. Nell'elenco delle periferiche, selezionare tutte le periferiche per la scansione e fare clic su Aggiungi.



Pianifica analisi

6. Al termine della programmazione, fare clic su Salva modifiche.

Le pianificazioni delle analisi diagnostiche e della raccolta dei dati di inventario possono essere modificate ed eliminate dalla pagina Raccolta dati.



Raccolta dei dati con le opzioni di pianificazione Modifica ed Elimina

Implementazione e configurazione della rete

Selezionare una delle seguenti opzioni per distribuire l'agente cloud CX:

- Per selezionare VMware vSphere/vCenter Thick Client ESXi 5.5/6.0, passare a Thick Client
- Per selezionare VMware vSphere/vCenter Web Client ESXi 6.0, passare a Web Client o vSphere Center
- Per selezionare Oracle Virtual Box 5.2.30, passare a Oracle VM
- Per selezionare Microsoft Hyper-V, passare a Hyper-V

Implementazione dell'OVA

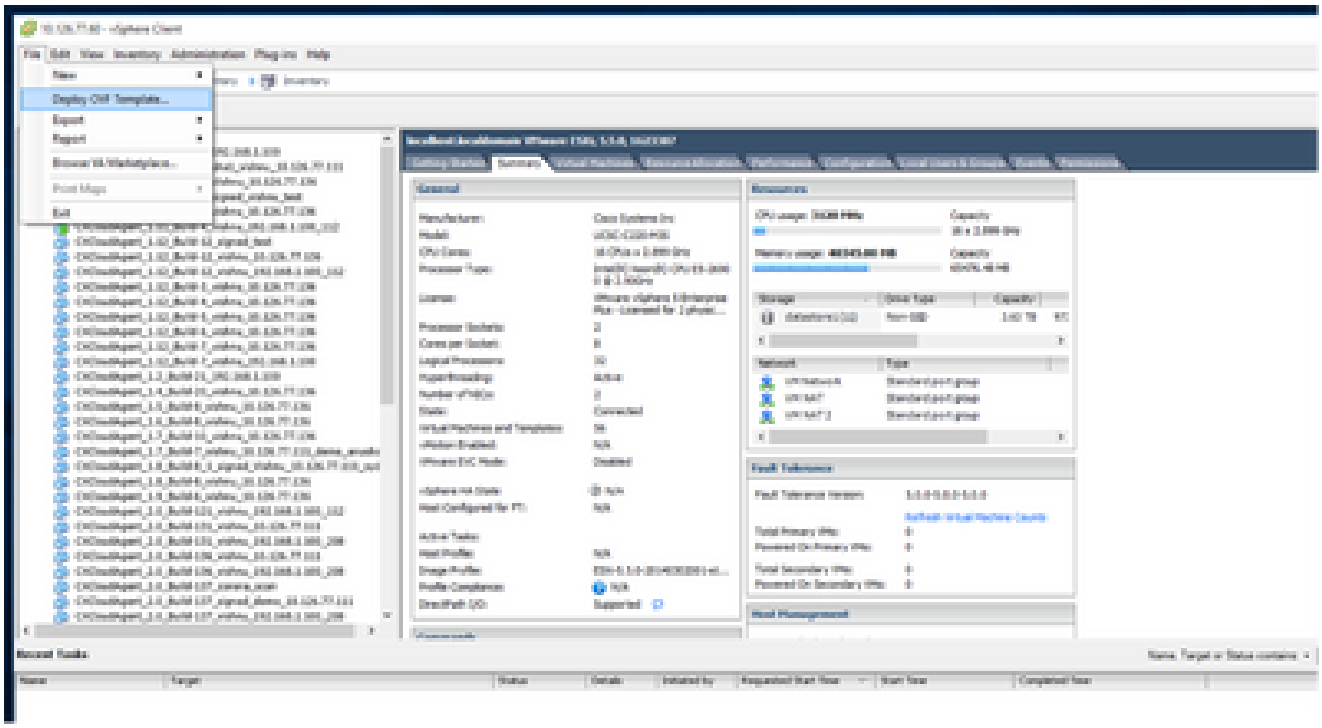
Installazione del thick client ESXi 5.5/6.0

Questo client consente la distribuzione di VSA agente cloud CX mediante il client thick vSphere.

1. Dopo aver scaricato l'immagine, avviare il client VMware vSphere ed eseguire il login.

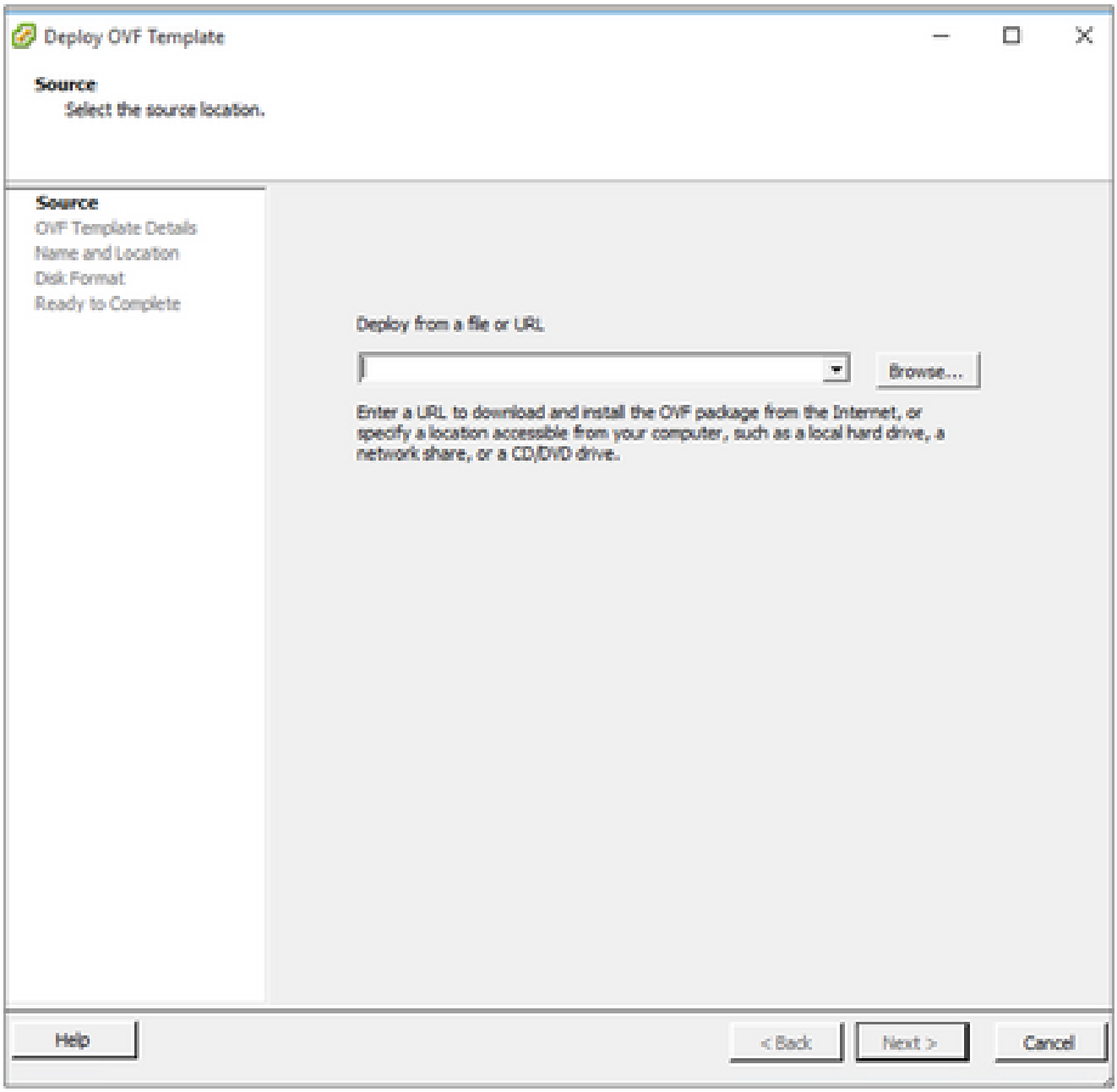
Accesso

2. Dal menu, selezionare File > Distribuisci modello OVF.



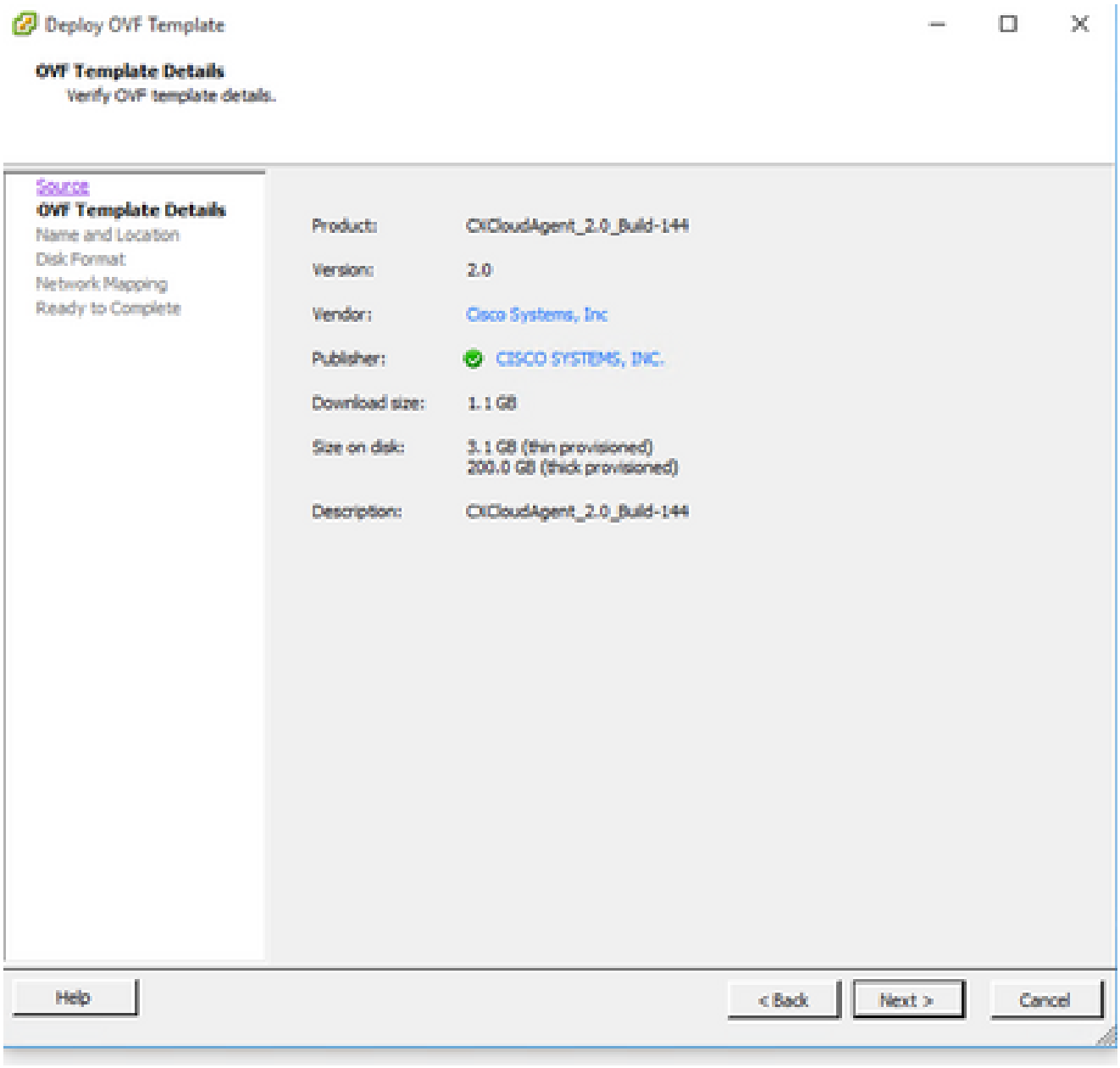
Client vSphere

3. Individuare e selezionare il file OVA e fare clic su Avanti.



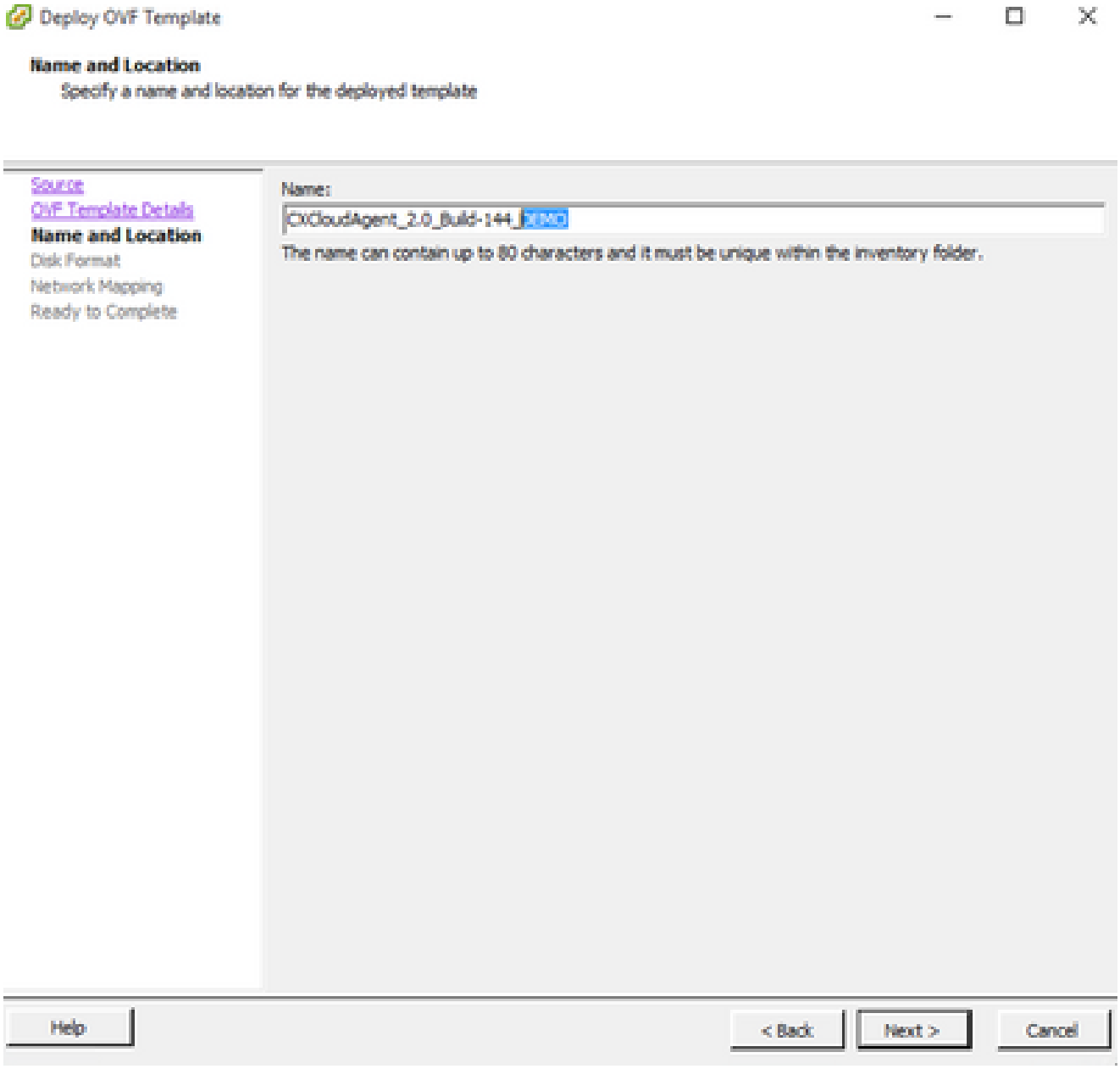
Percorso OVA

4. Verificare i dettagli OVF e fare clic su Avanti.



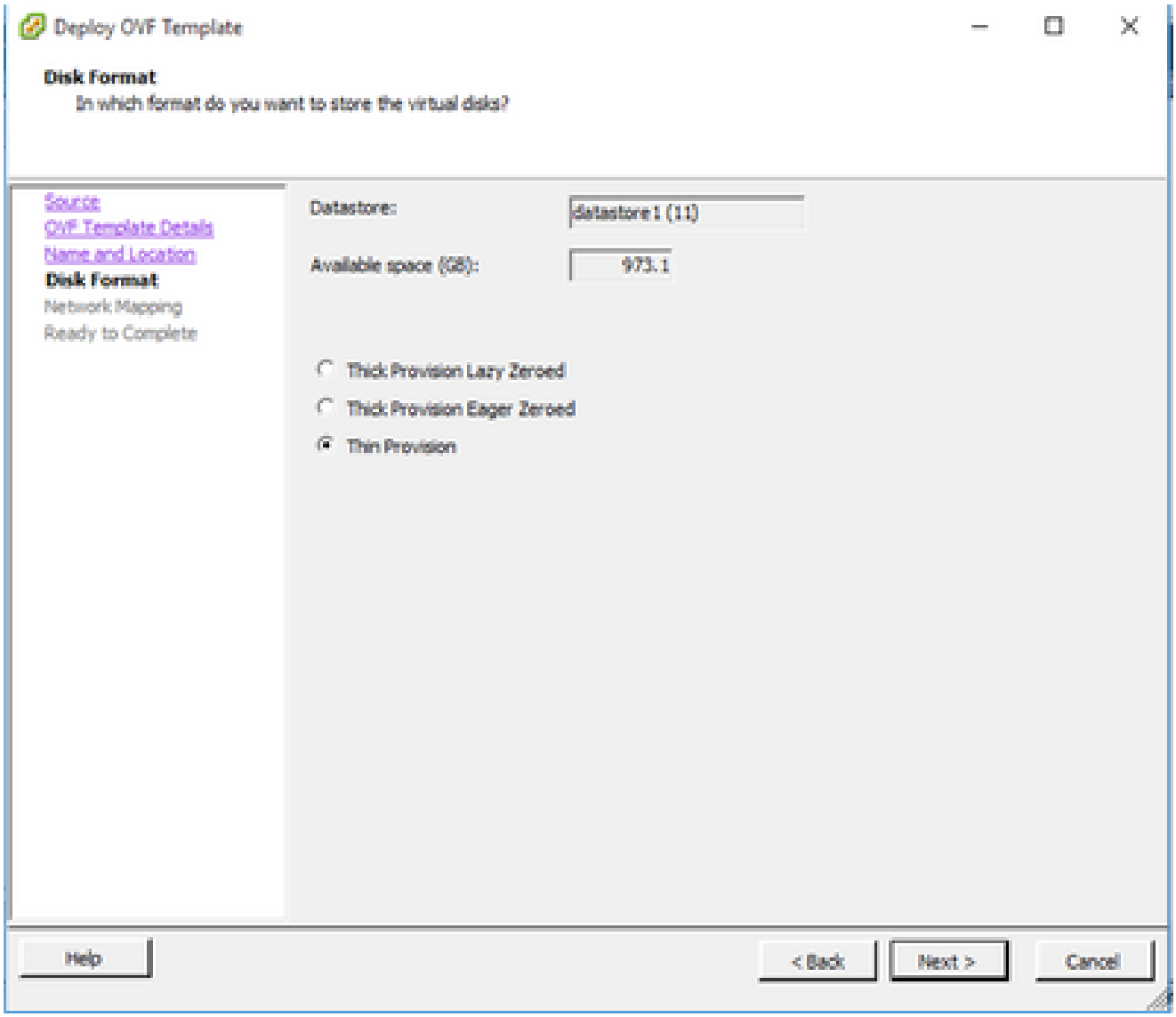
Dettagli del modello

5. Immettere un nome univoco e fare clic su Avanti.



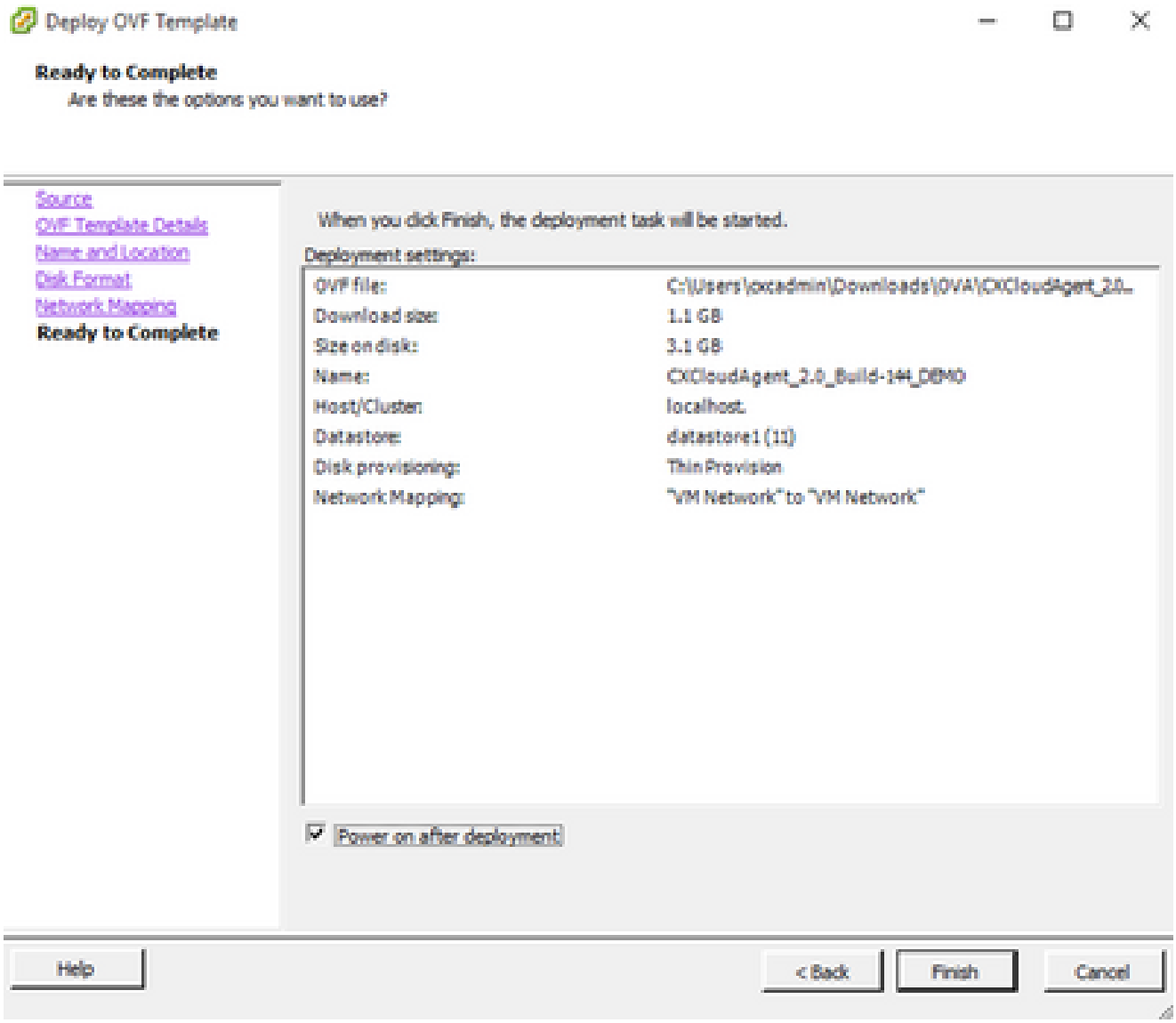
Nome e posizione

6. Selezionare un formato disco e fare clic su Avanti (si consiglia il thin provisioning).



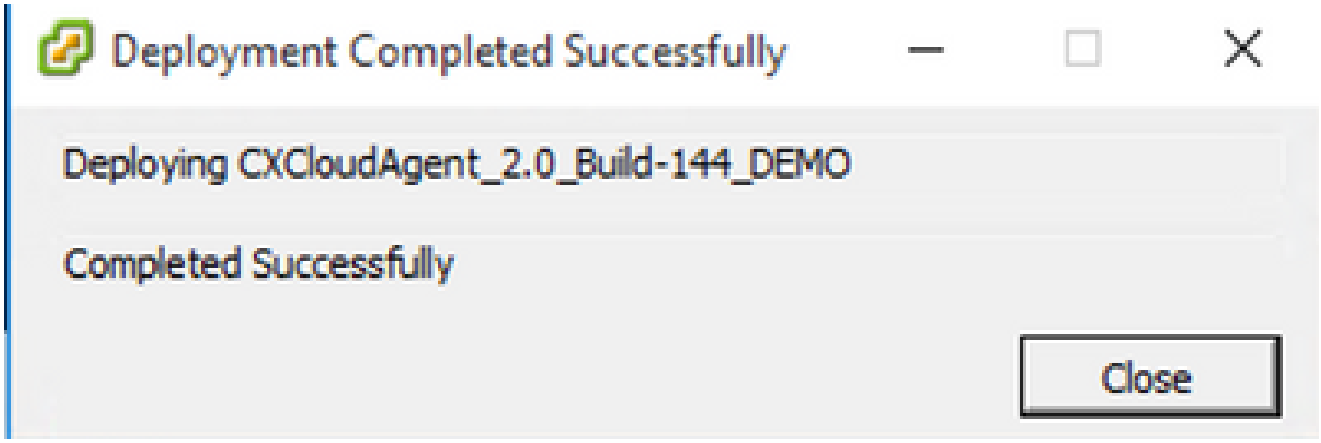
Formato del disco

7. Selezionare la casella di controllo Accendi dopo la distribuzione e fare clic su Chiudi.



Pronto per il completamento

L'installazione può richiedere alcuni minuti. Al completamento della distribuzione viene visualizzata la conferma.



Distribuzione completata

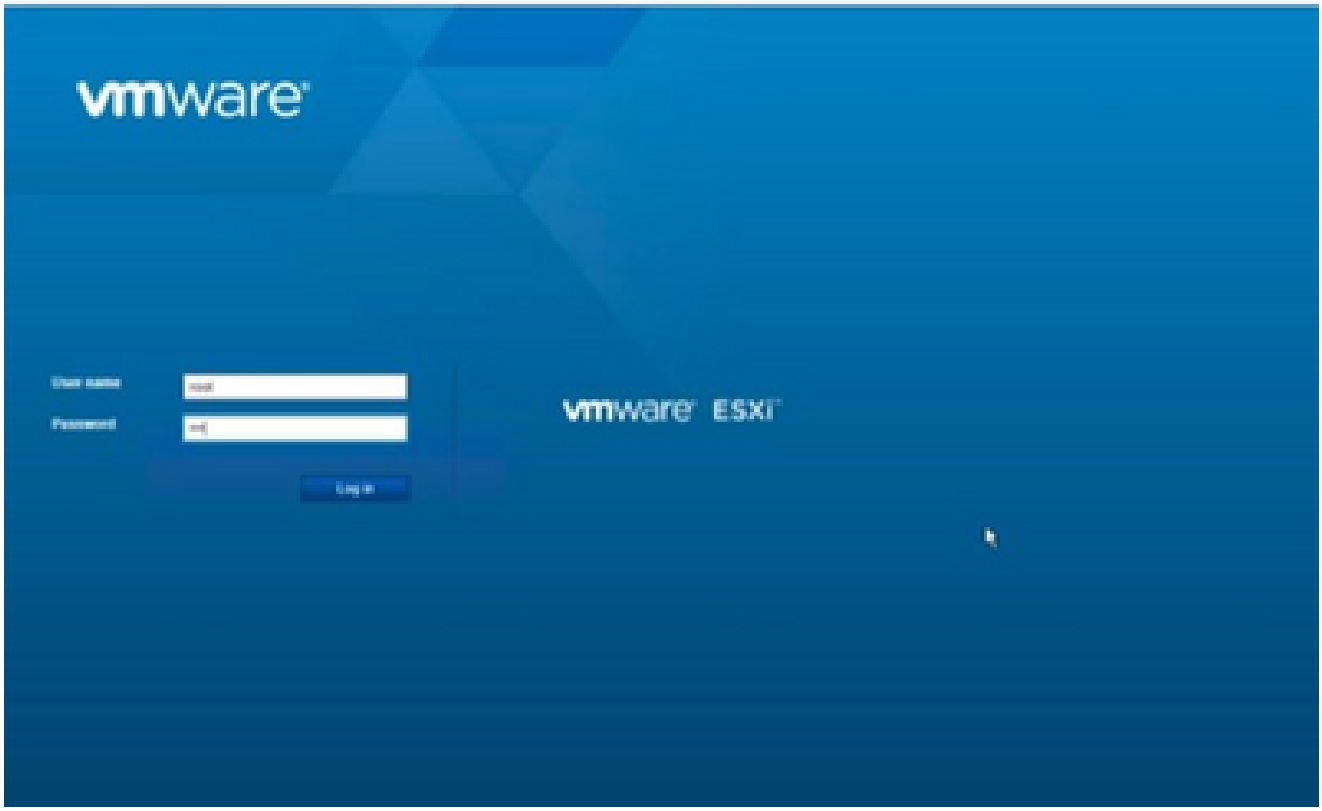
8. Selezionare la VM distribuita, aprire la console e passare a Configurazione di rete per

procedere con i passaggi successivi.

Installazione del client Web ESXi 6.0

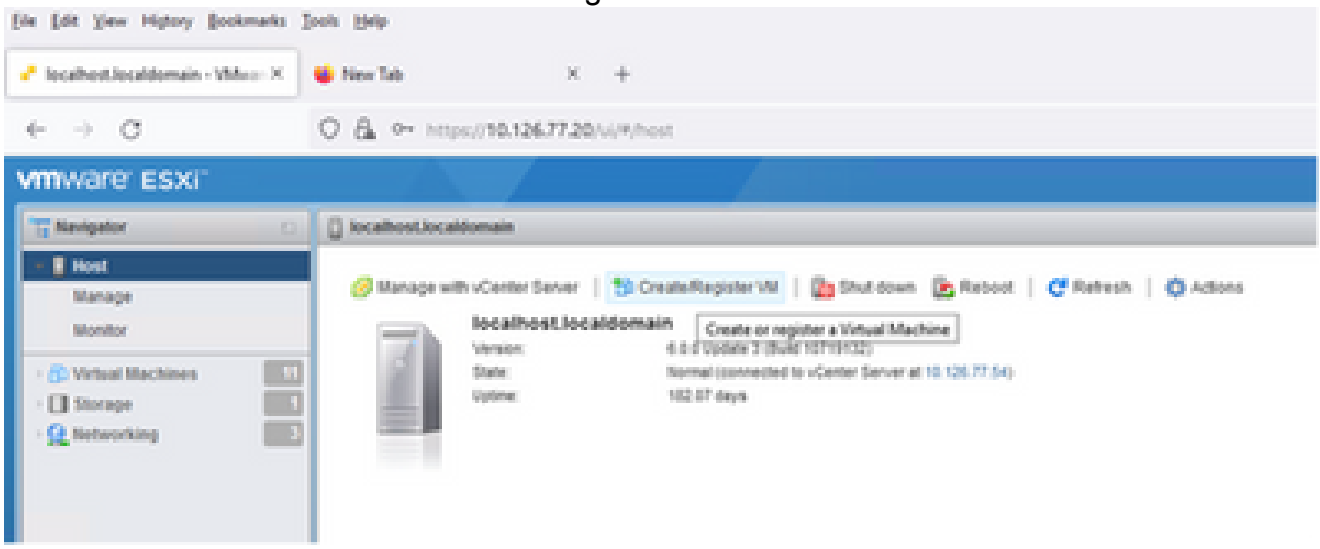
Questo client distribuisce l'agente cloud CX tramite il Web vSphere.

1. Accedere all'interfaccia utente di VMWare con le credenziali ESXi/hypervisor utilizzate per l'installazione della VM.



Accesso a VMware ESXi

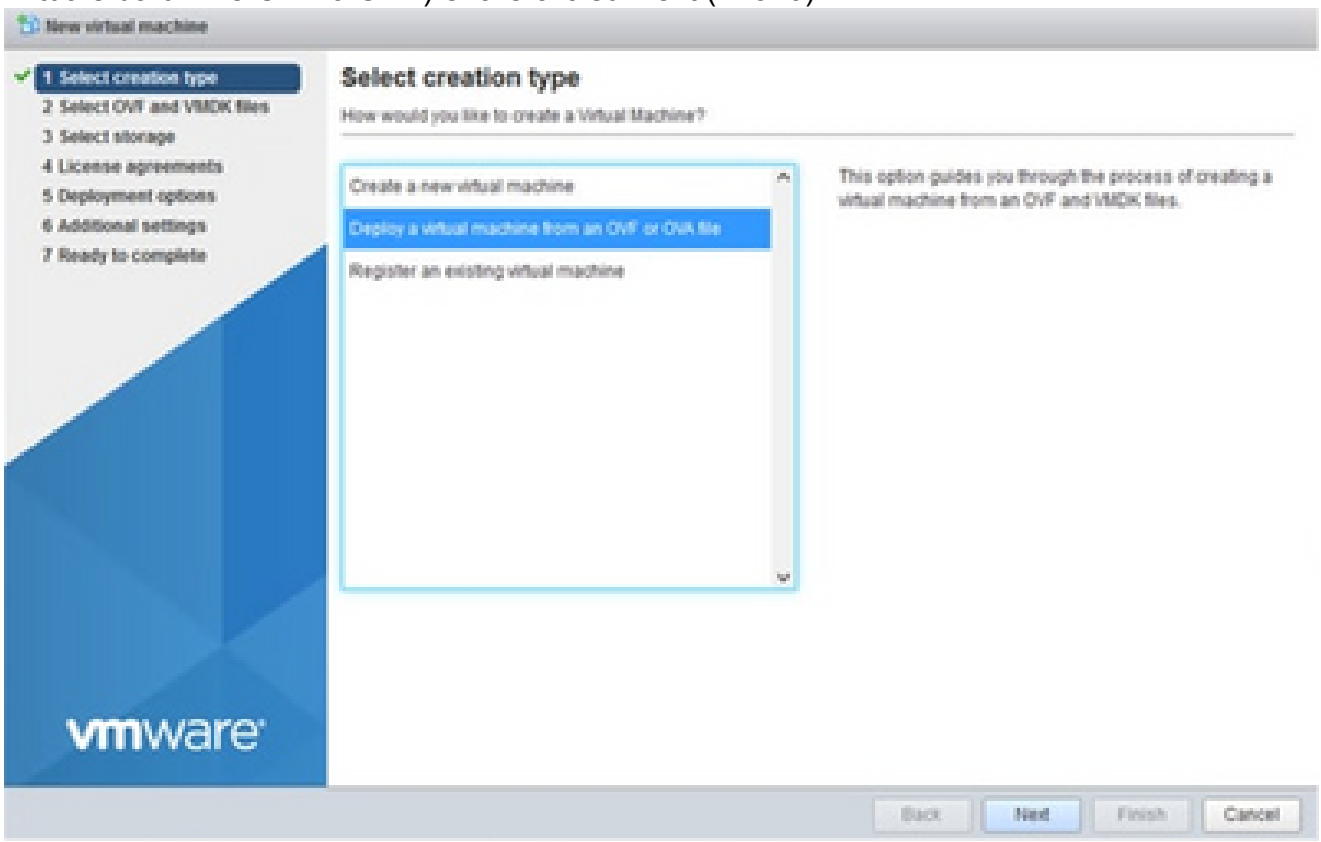
2. Selezionare Virtual Machine > Create/Register VM.



Creazione della VM

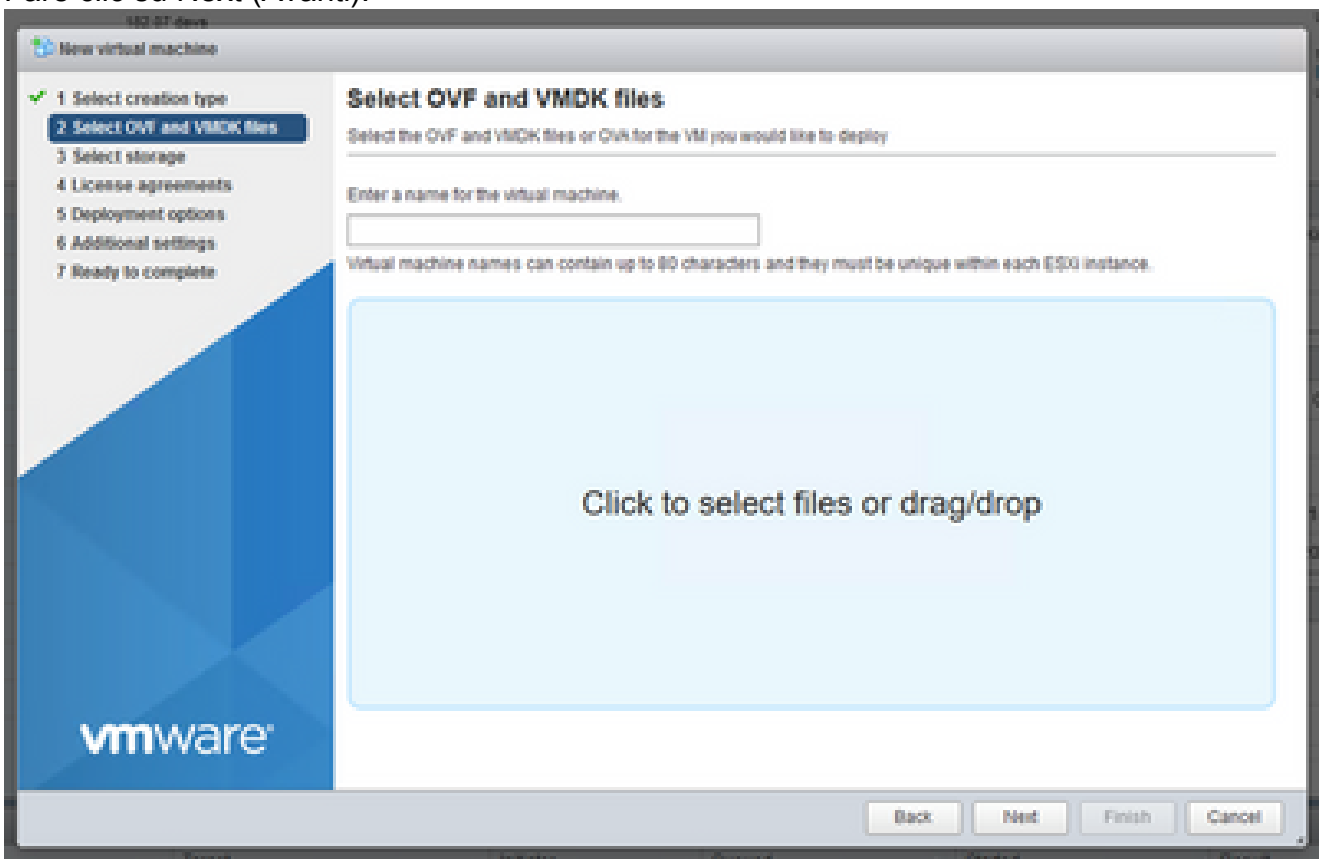
3. Selezionare Deploy a virtual machine from an OVF or OVA file (Implementa una macchina

virtuale da un file OVF o OVA) e fare clic su Next (Avanti).



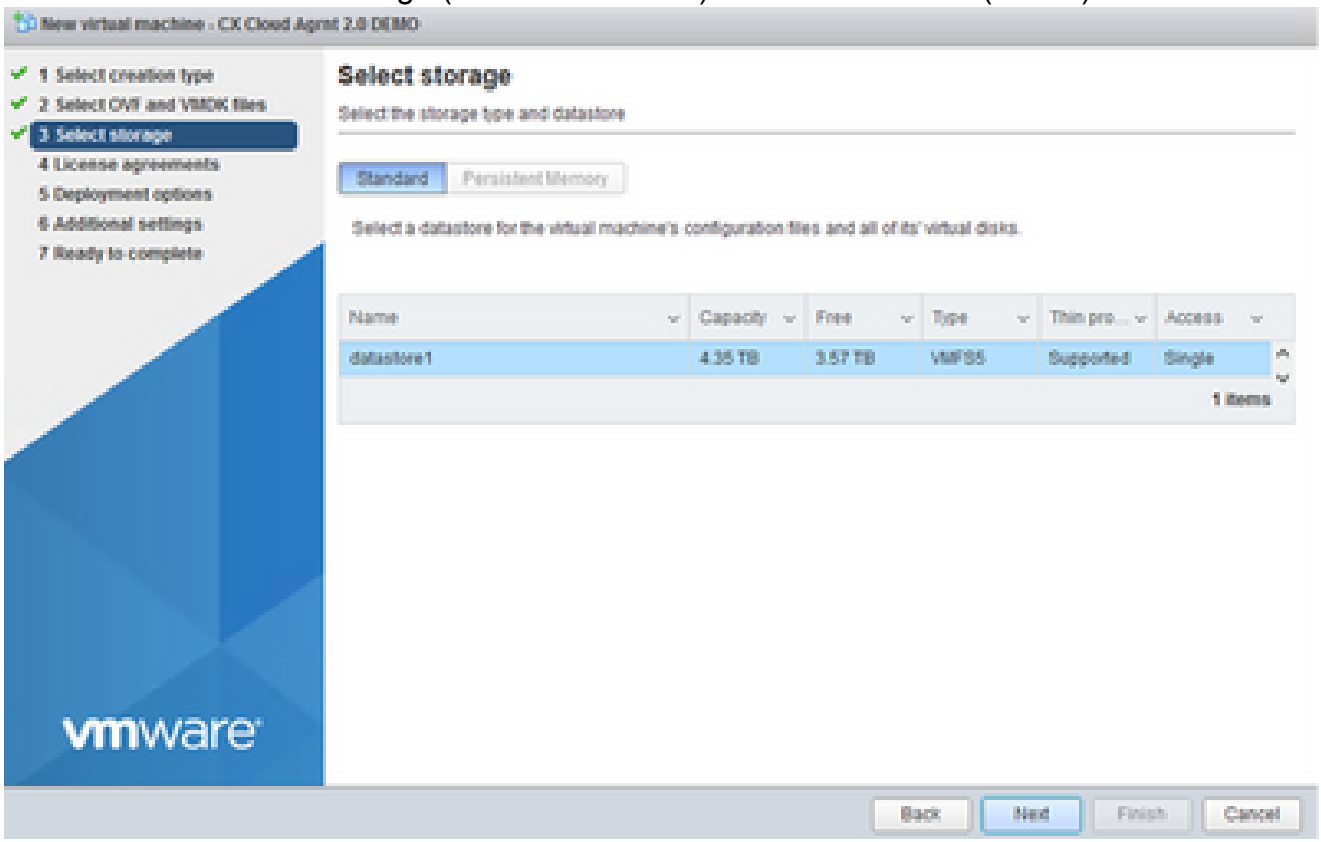
Seleziona tipo di creazione

4. Immettere il nome della macchina virtuale, selezionare il file o trascinare il file OAV scaricato.
5. Fare clic su Next (Avanti).



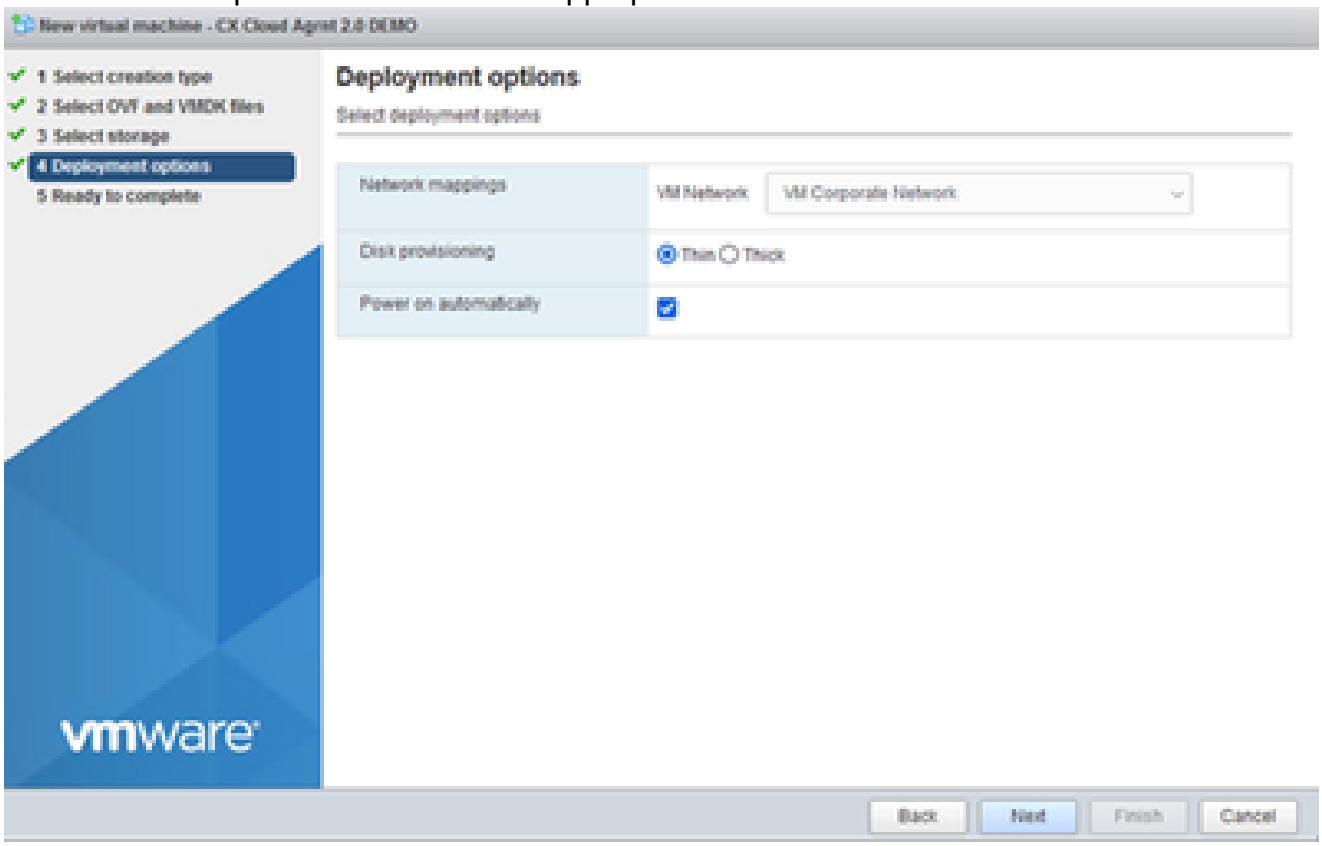
Selezione dell'OVA

6. Selezionare Standard Storage (Archivio standard) e fare clic su Next (Avanti).

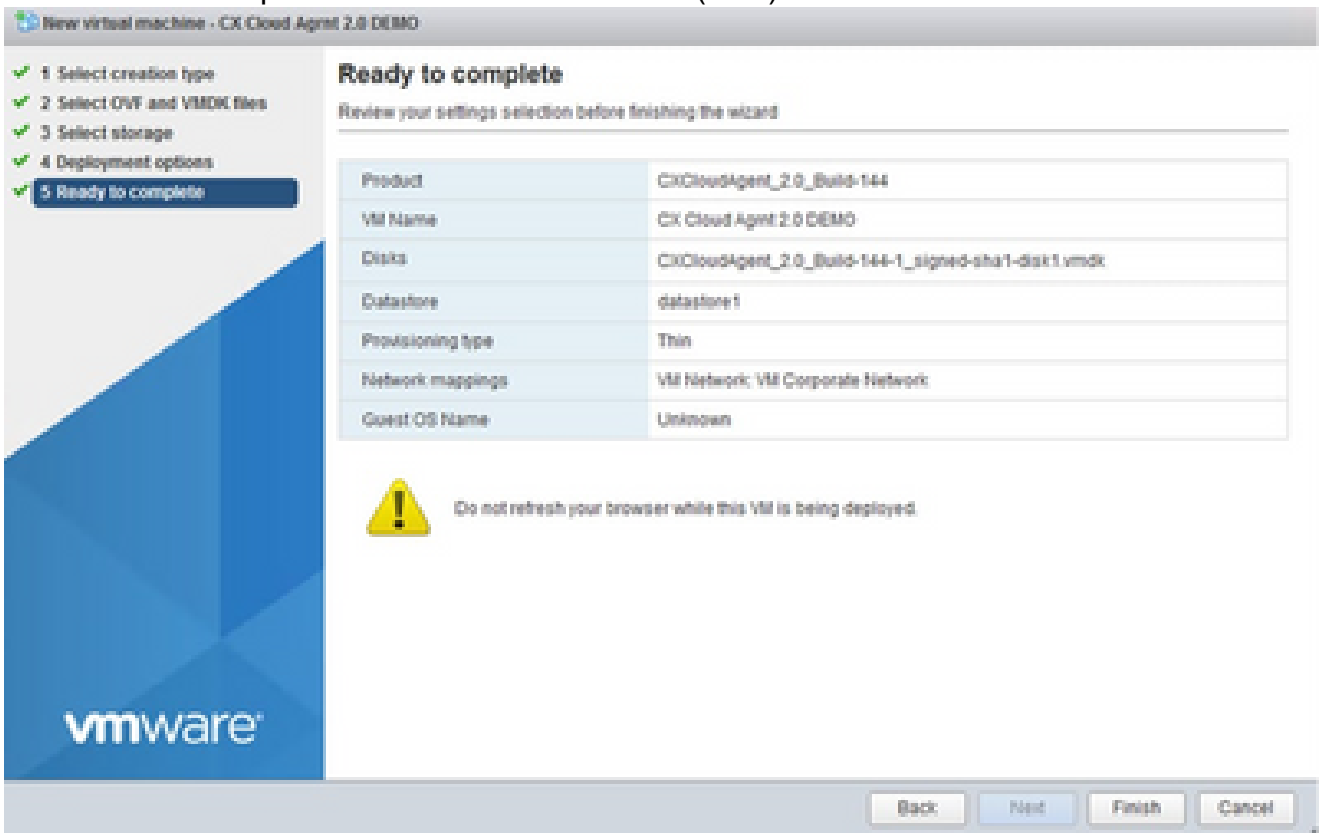


Selezione dell'archivio

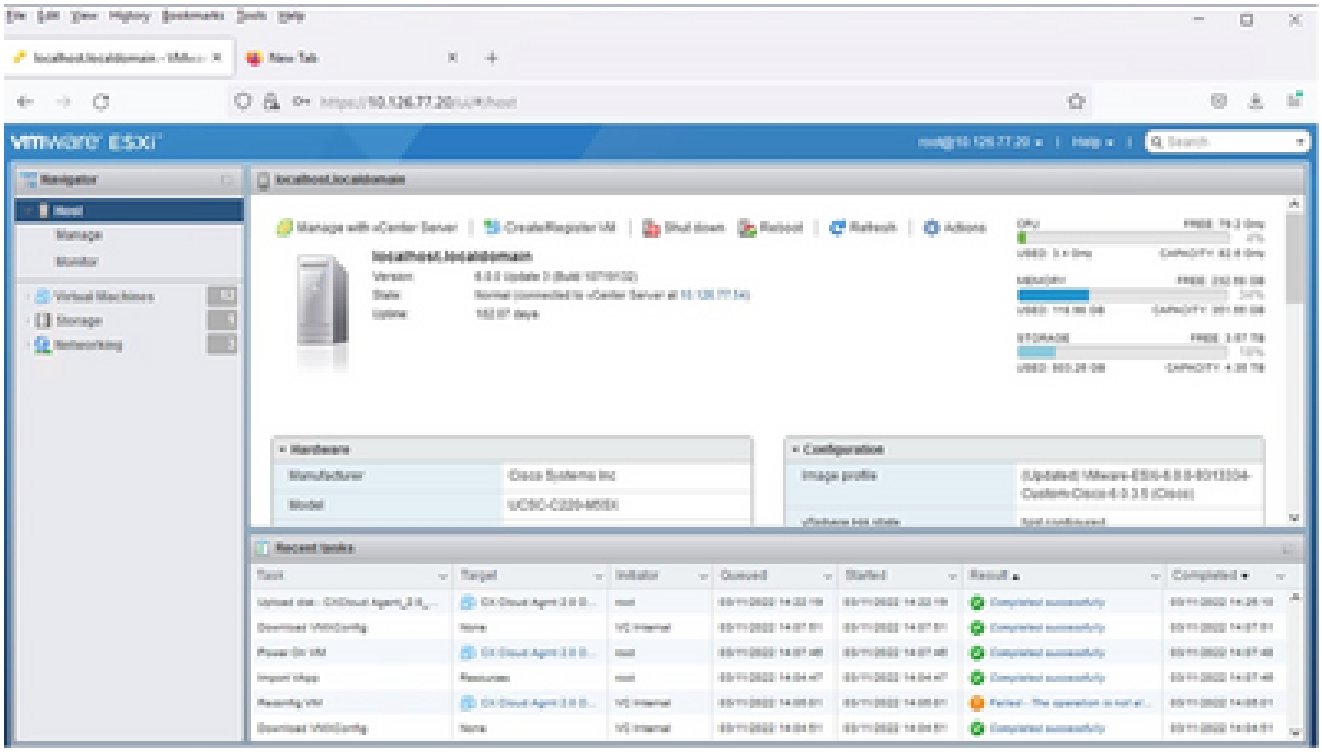
7. Selezionare le opzioni di distribuzione appropriate e fare clic su Avanti.



8. Riesaminare le impostazioni e fare clic su Finish (Fine).

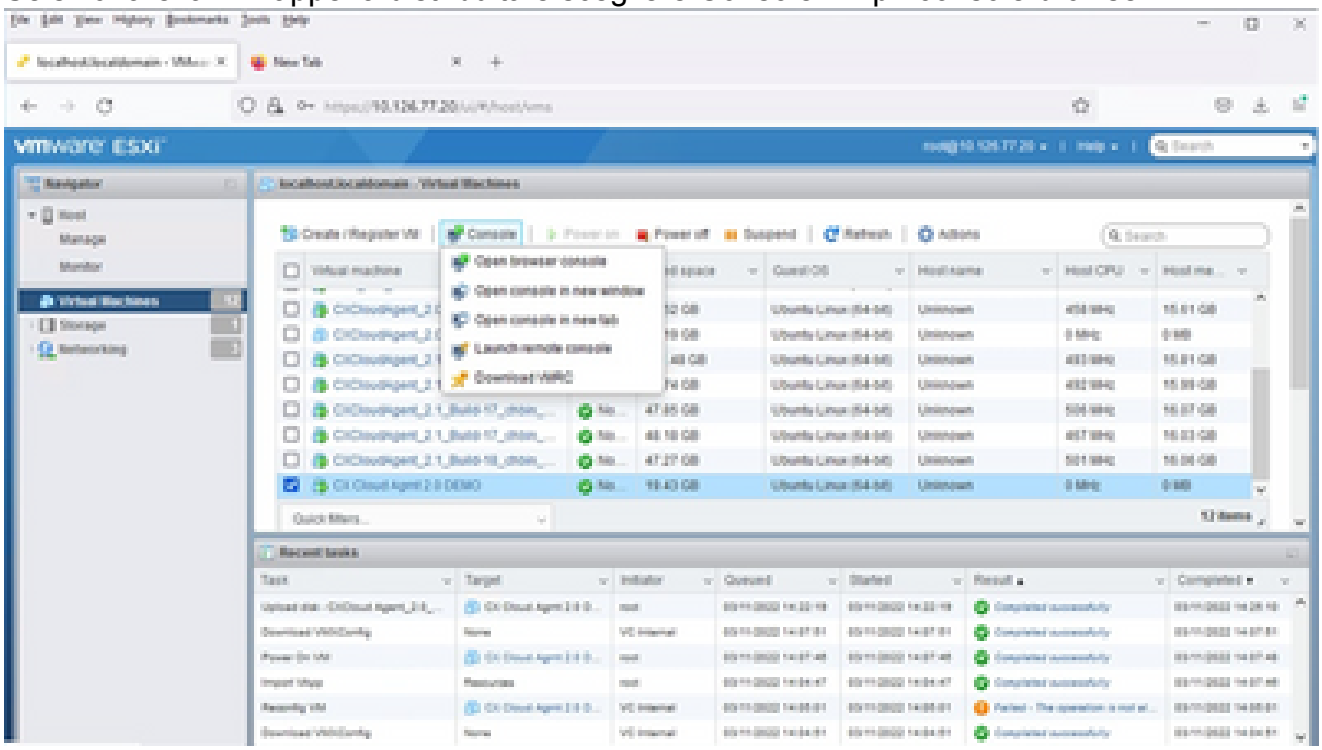


Pronto per il completamento



Procedura completata

9. Selezionare la VM appena distribuita e scegliere Console > Apri console browser.



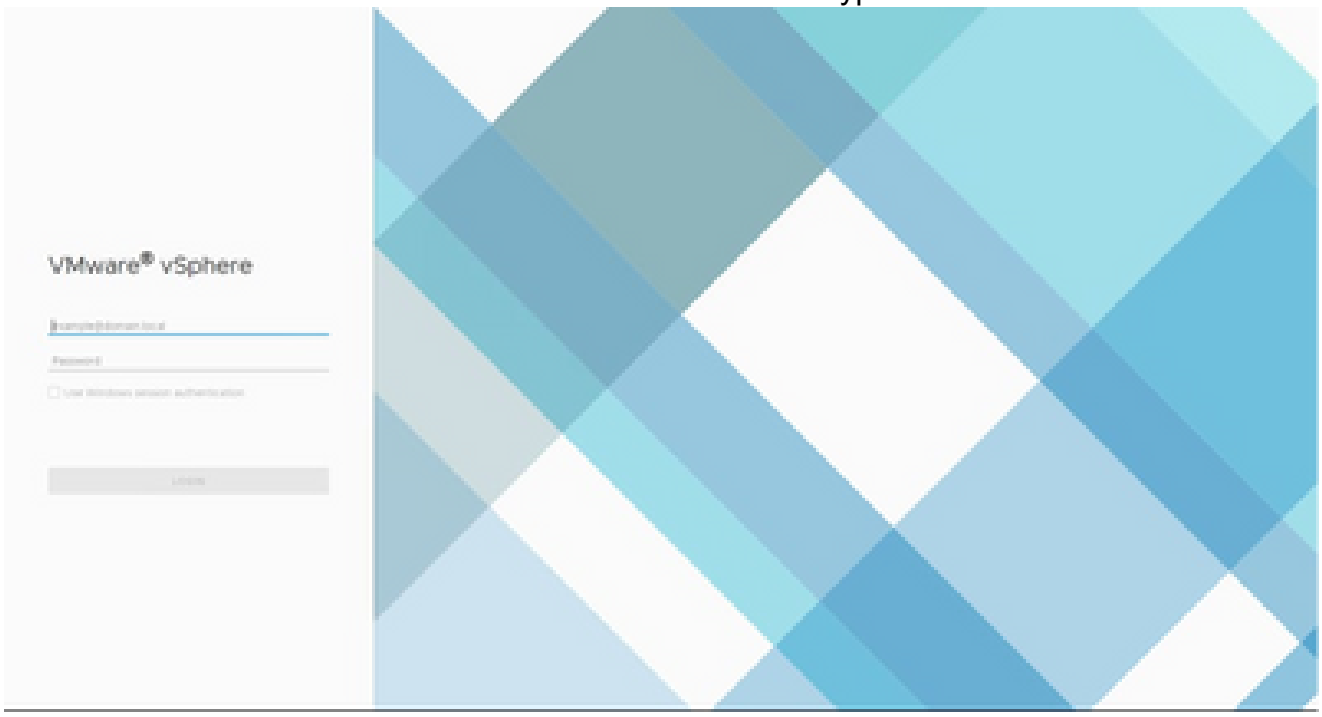
Console

10. Passare a Configurazione di rete per continuare con i passaggi successivi.

Installazione del client Web vCenter

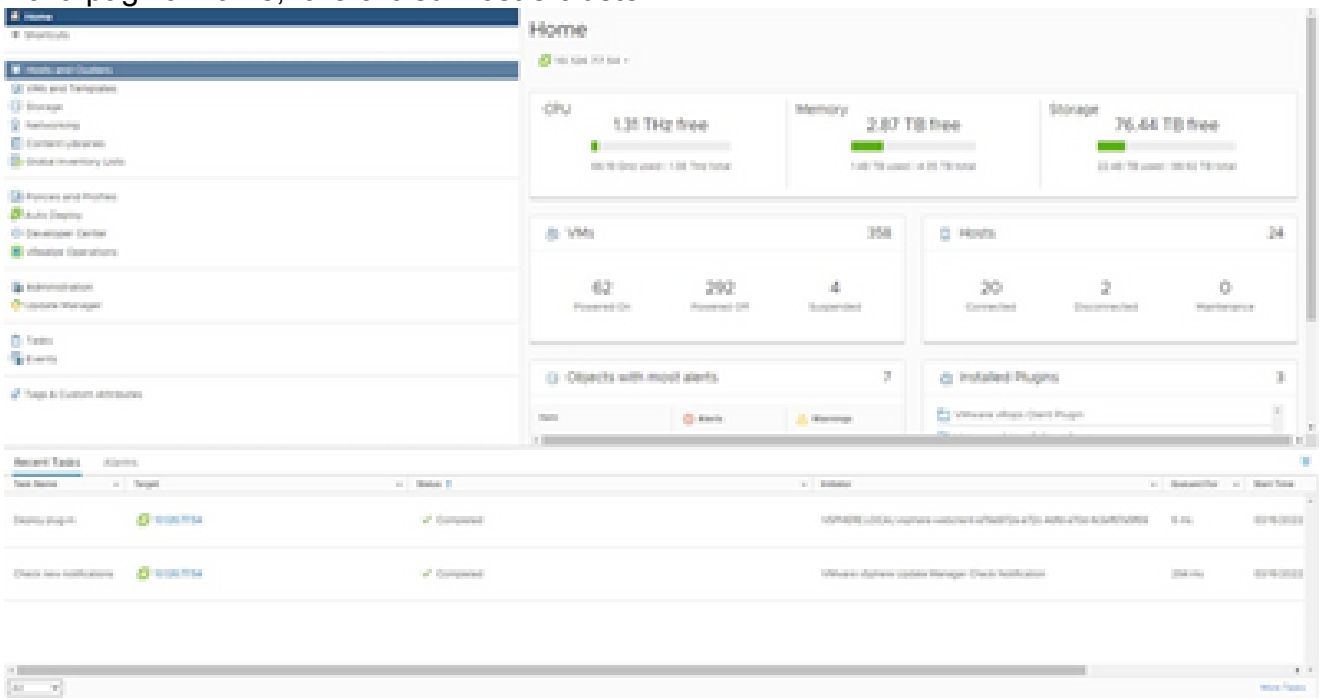
Eseguire questa procedura:

1. Accedere al client vCenter utilizzando le credenziali ESXi/hypervisor.



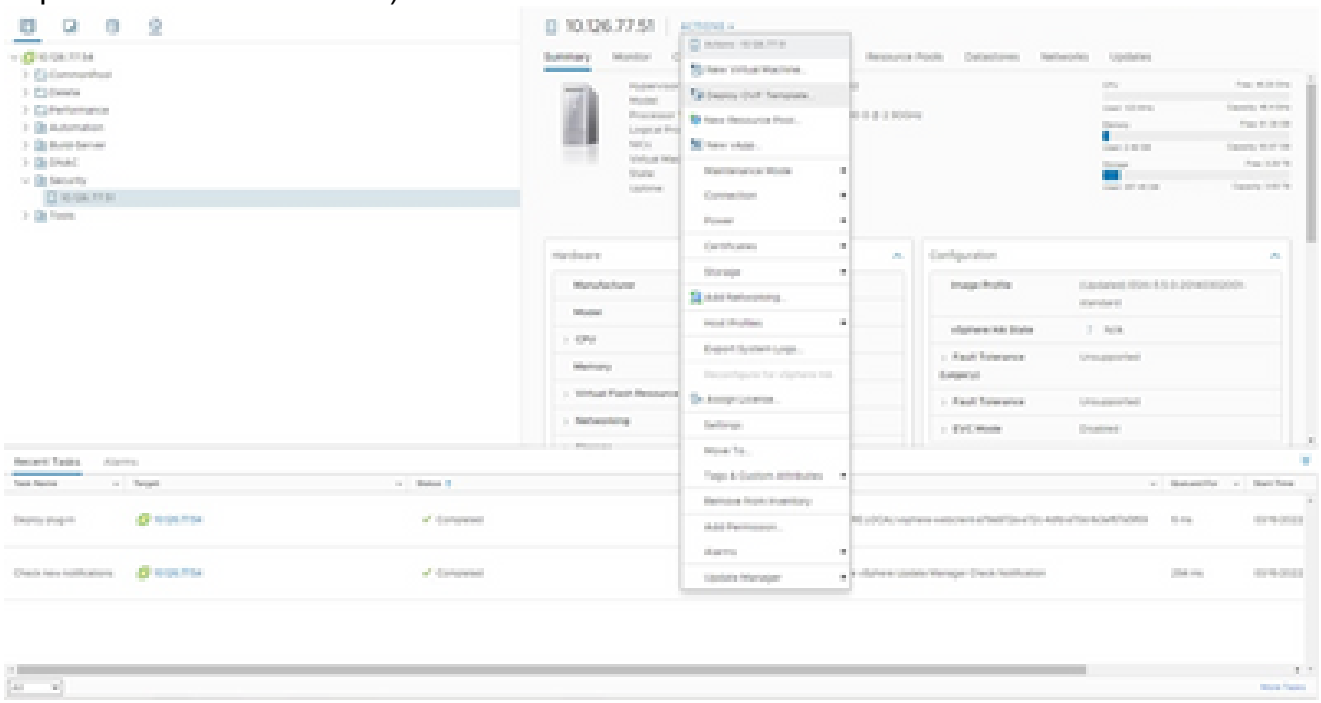
Accedi

2. Dalla pagina Home, fare clic su Host e cluster.

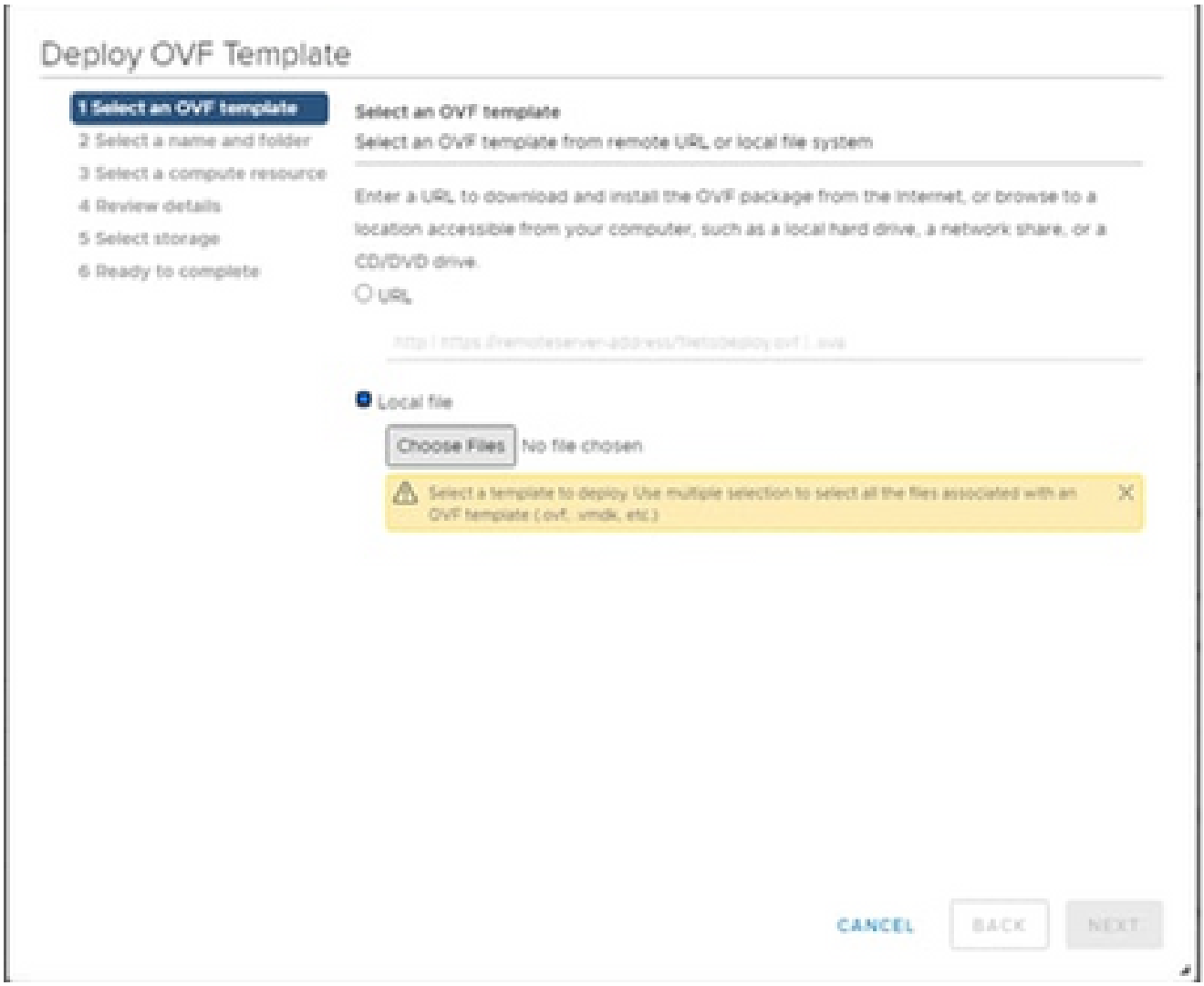


Home page

3. Selezionare la macchina virtuale e fare clic su Action > Deploy OVF Template (Azione > Implementa il modello OVF).

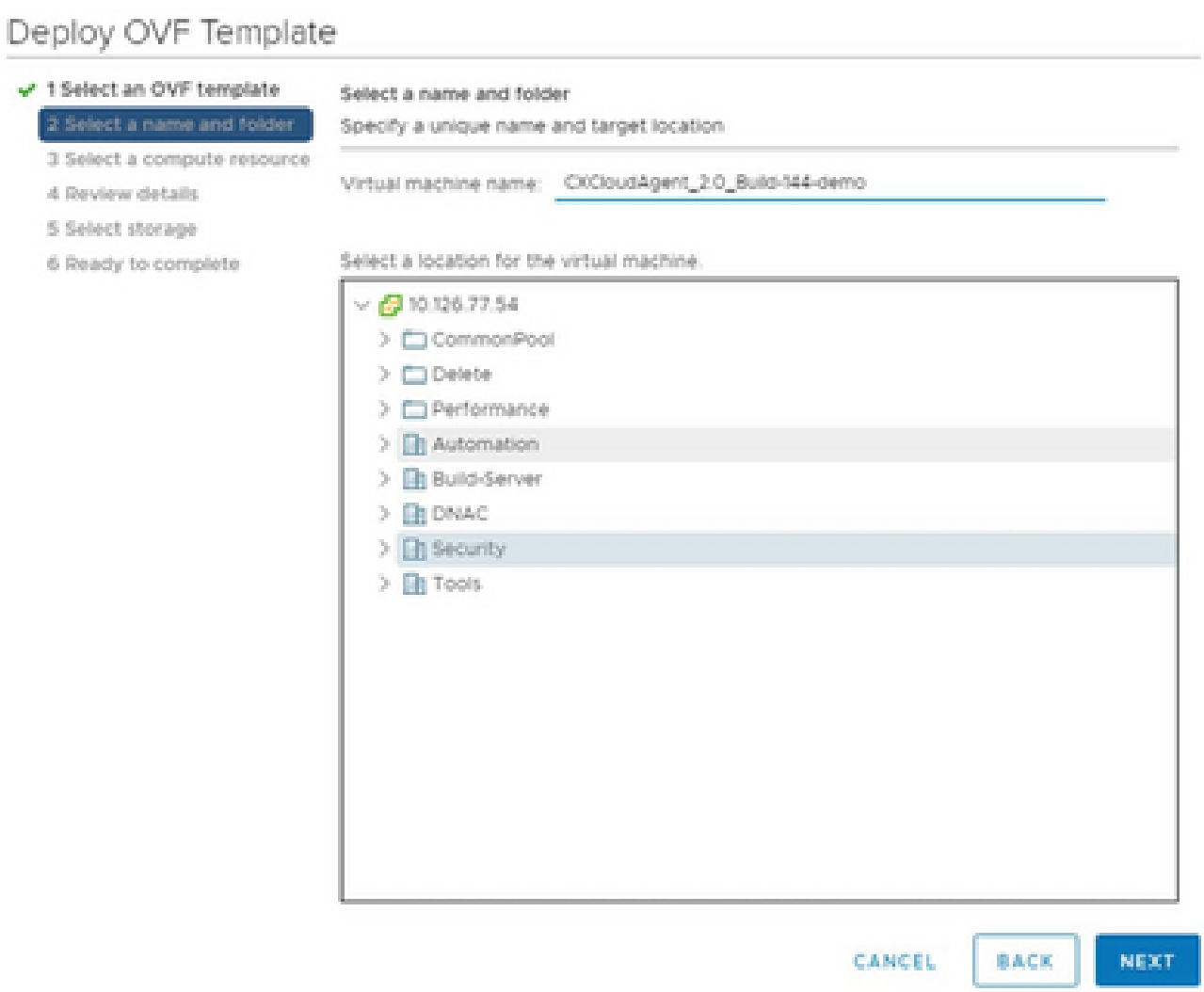


Azioni



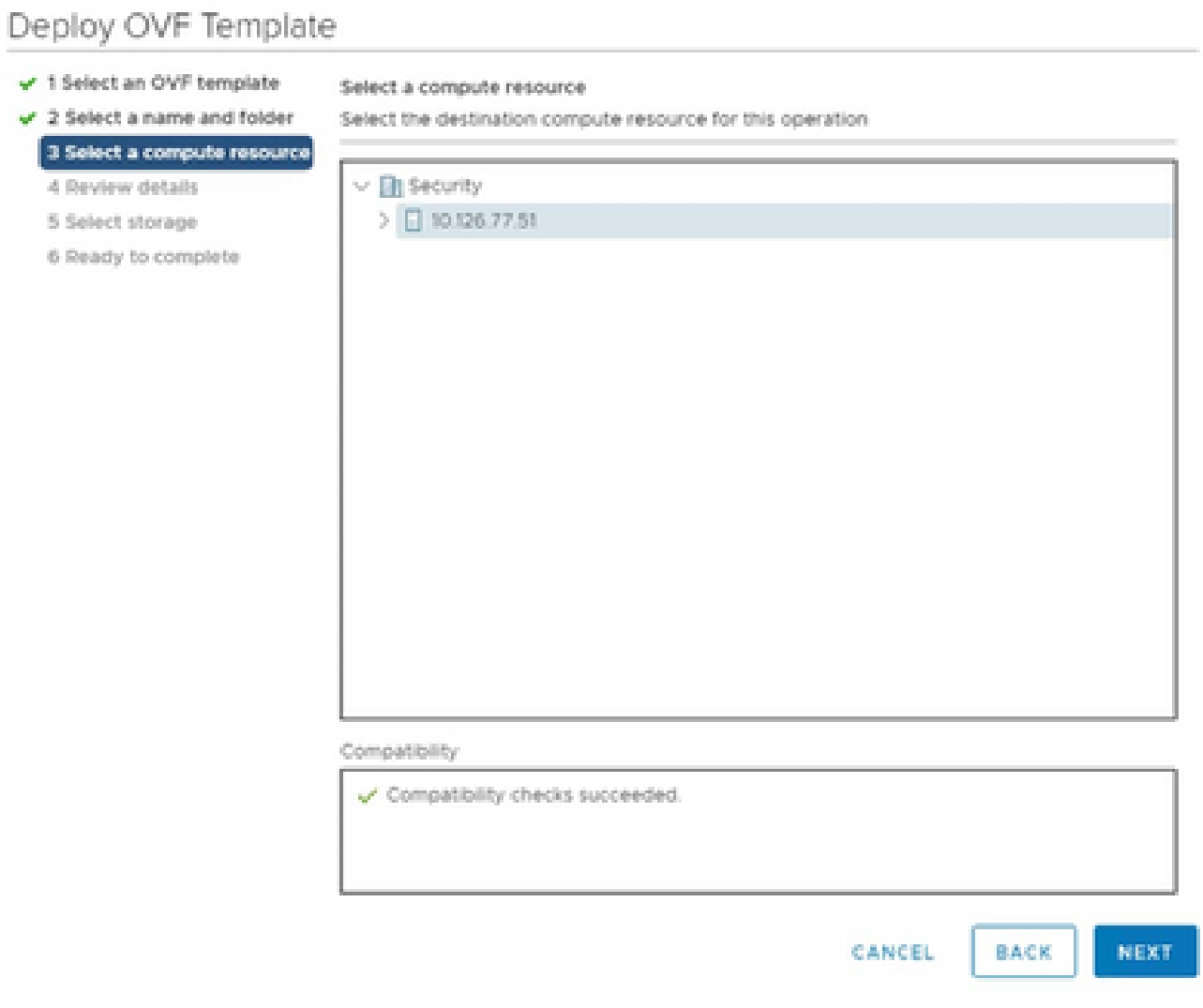
Selezione del modello

4. Aggiungere l'URL direttamente o selezionare il file OVA e fare clic su Avanti.
5. Se necessario, immettere un nome univoco e selezionare la posizione.
6. Fare clic su Next (Avanti).



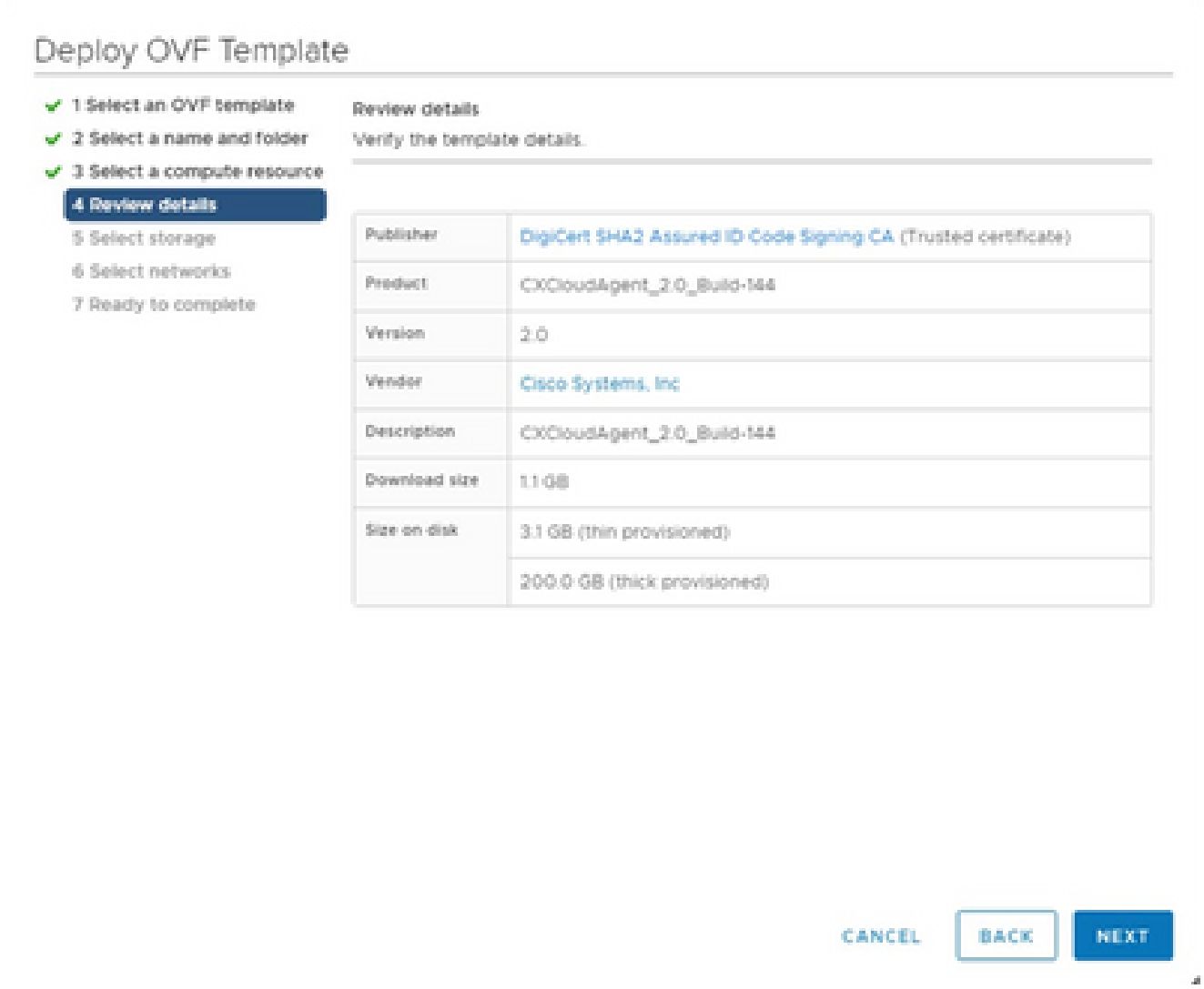
Nome e cartella

7. Selezionare una risorsa di calcolo e fare clic su Avanti.



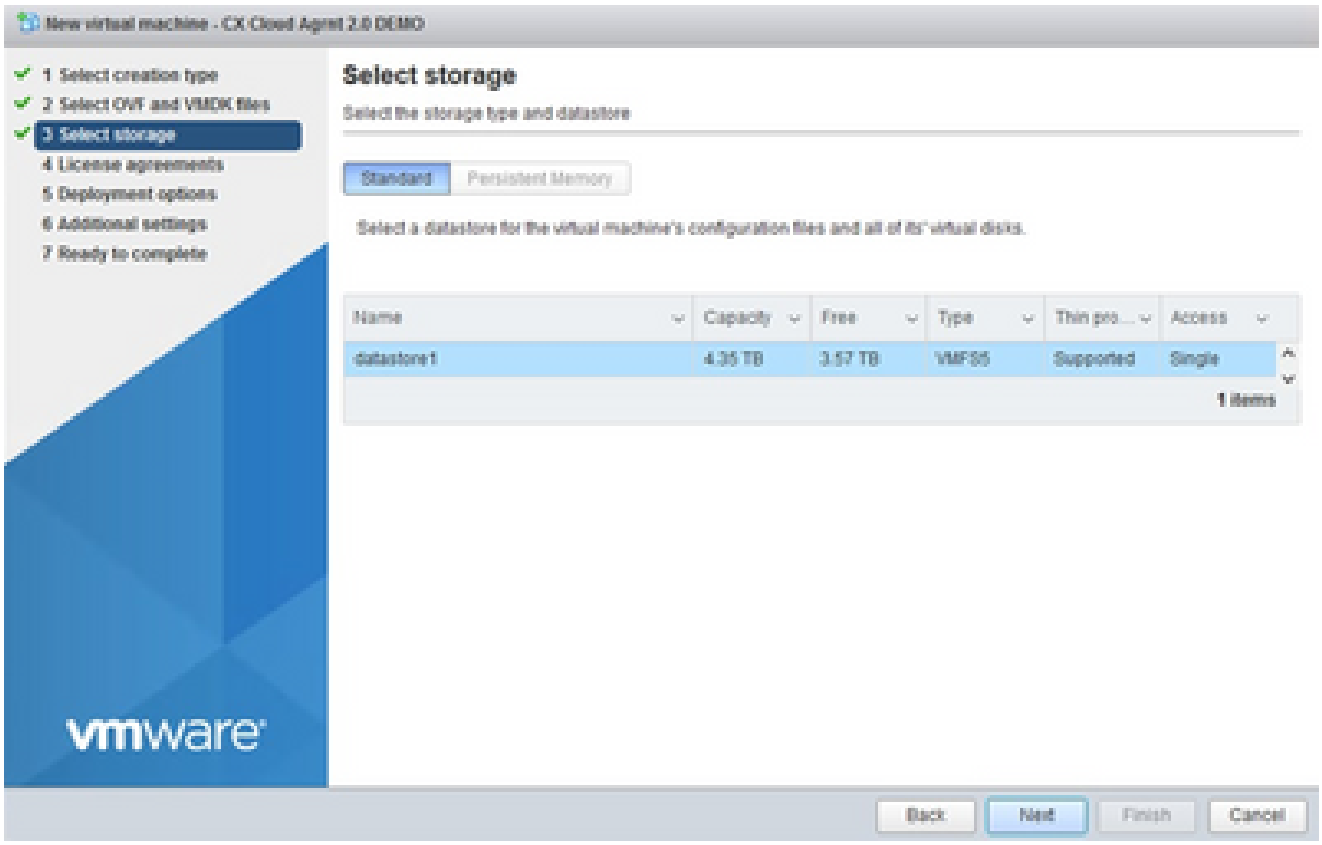
Seleziona risorsa computer

8. Riesaminare i dettagli e fare clic su Next (Avanti).



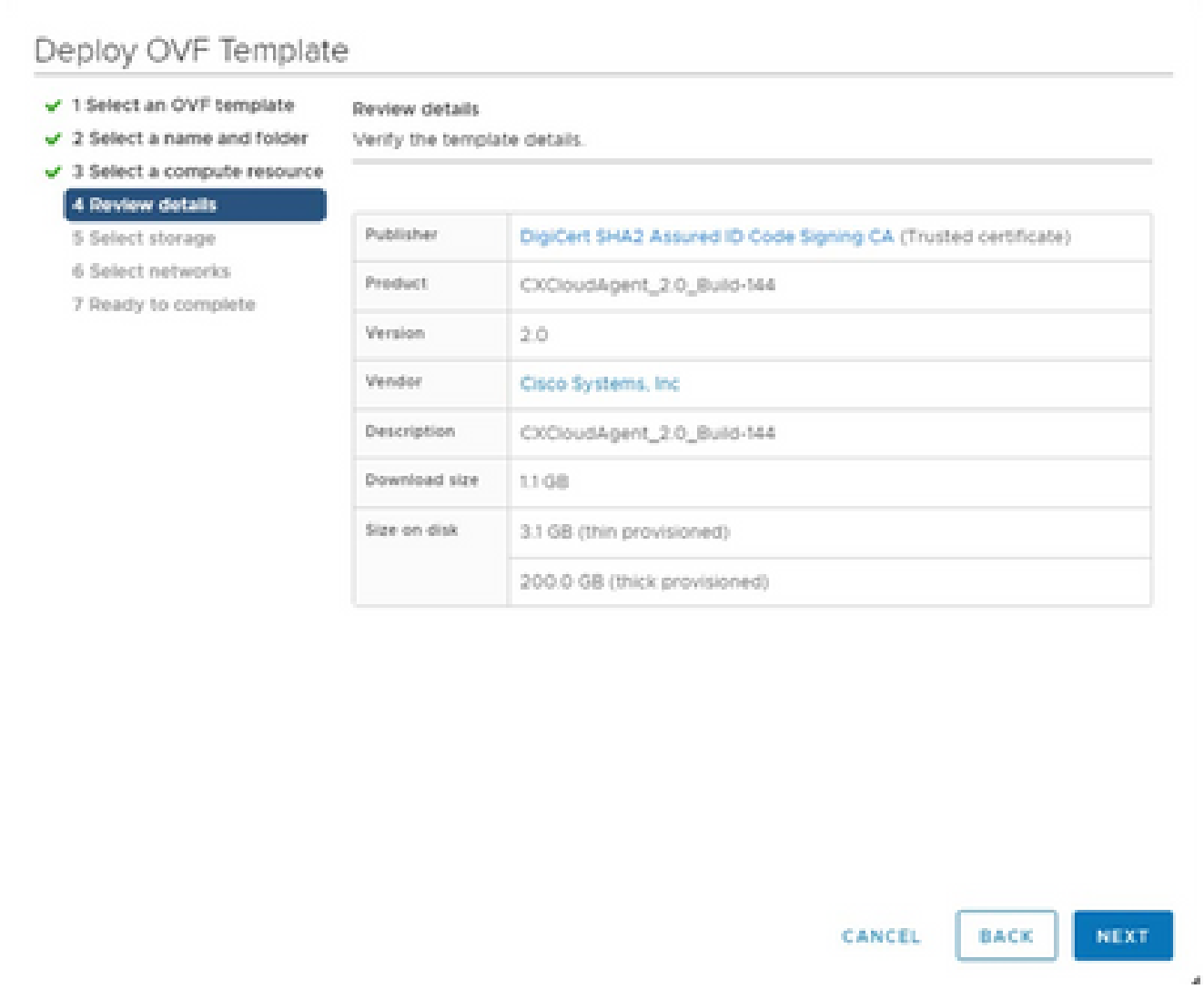
Riesame dei dettagli

9. Selezionare il formato del disco virtuale e fare clic su Next (Avanti).



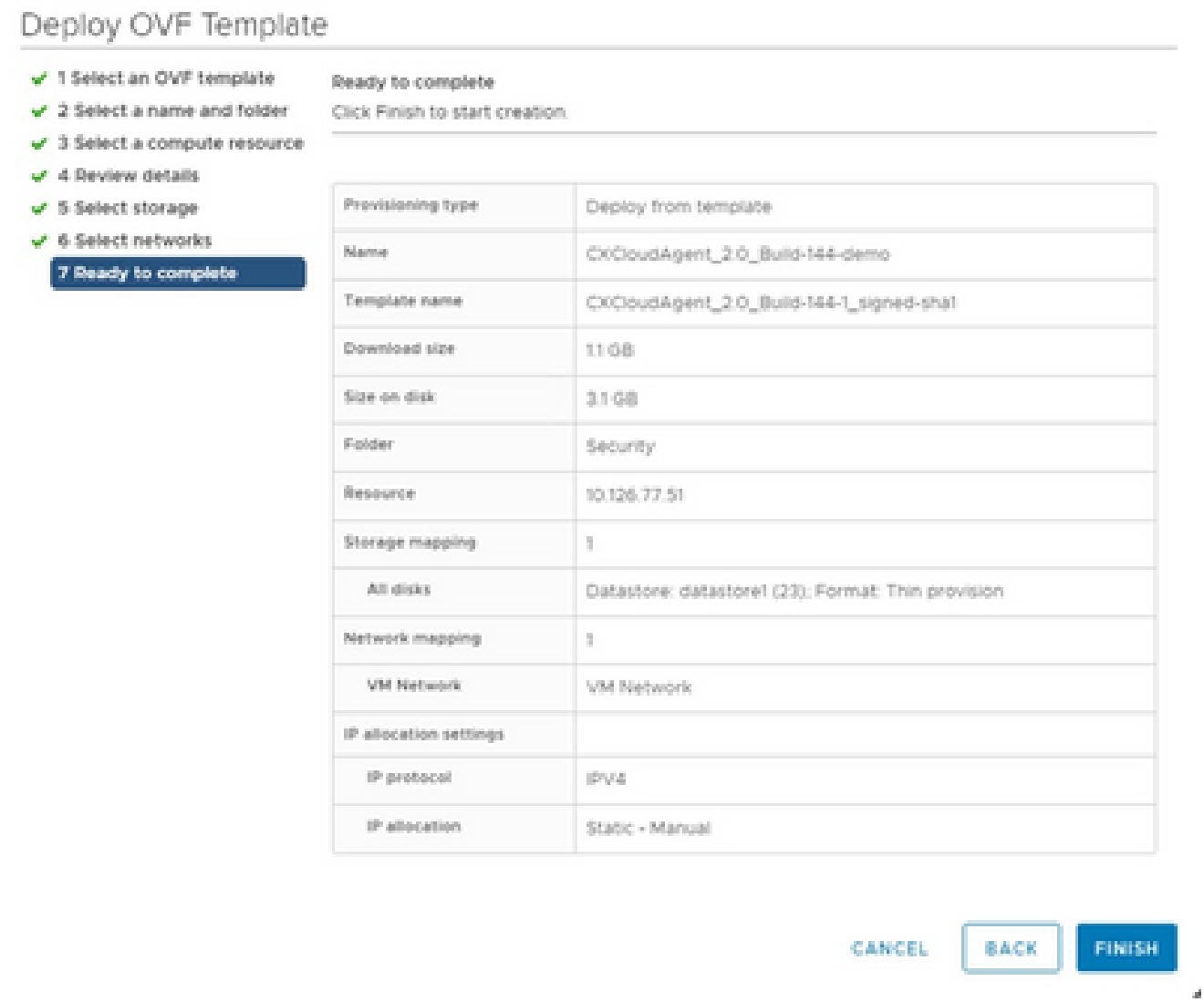
Selezione dell'archivio

10. Fare clic su Next (Avanti).



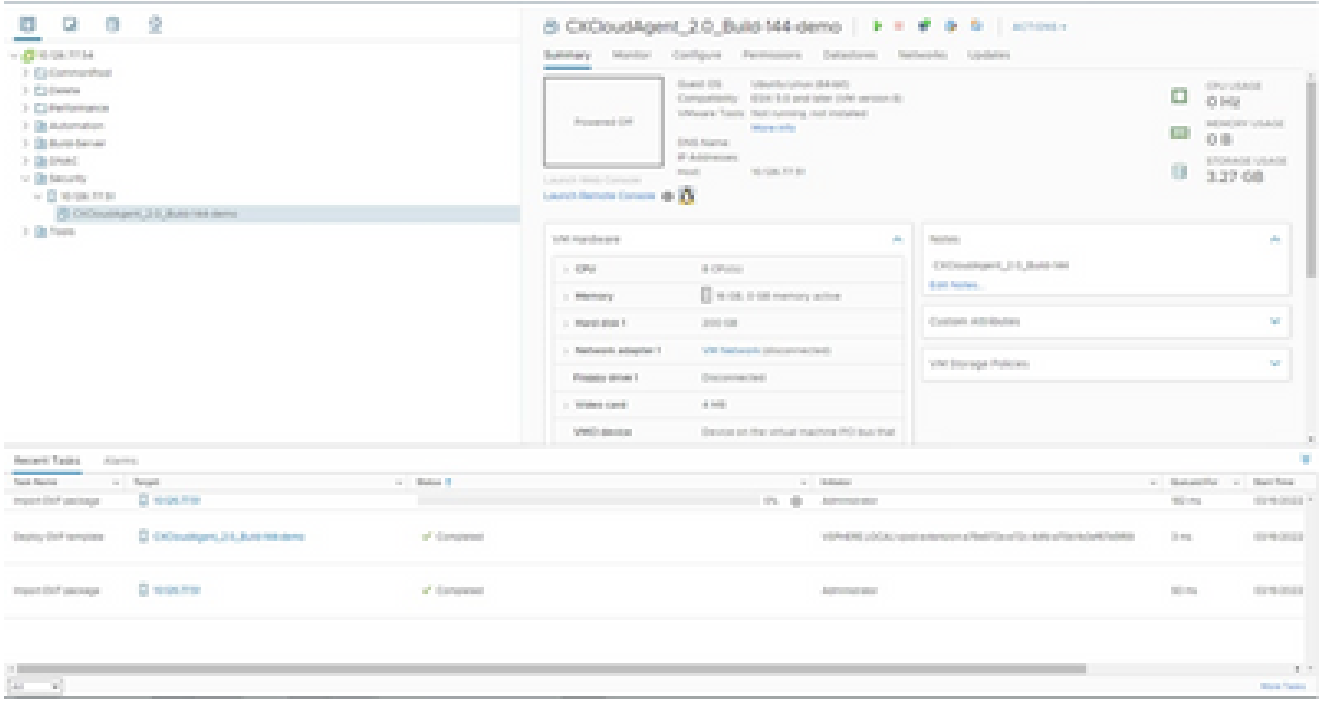
Seleziona rete

11. Fare clic su Finish (Fine).



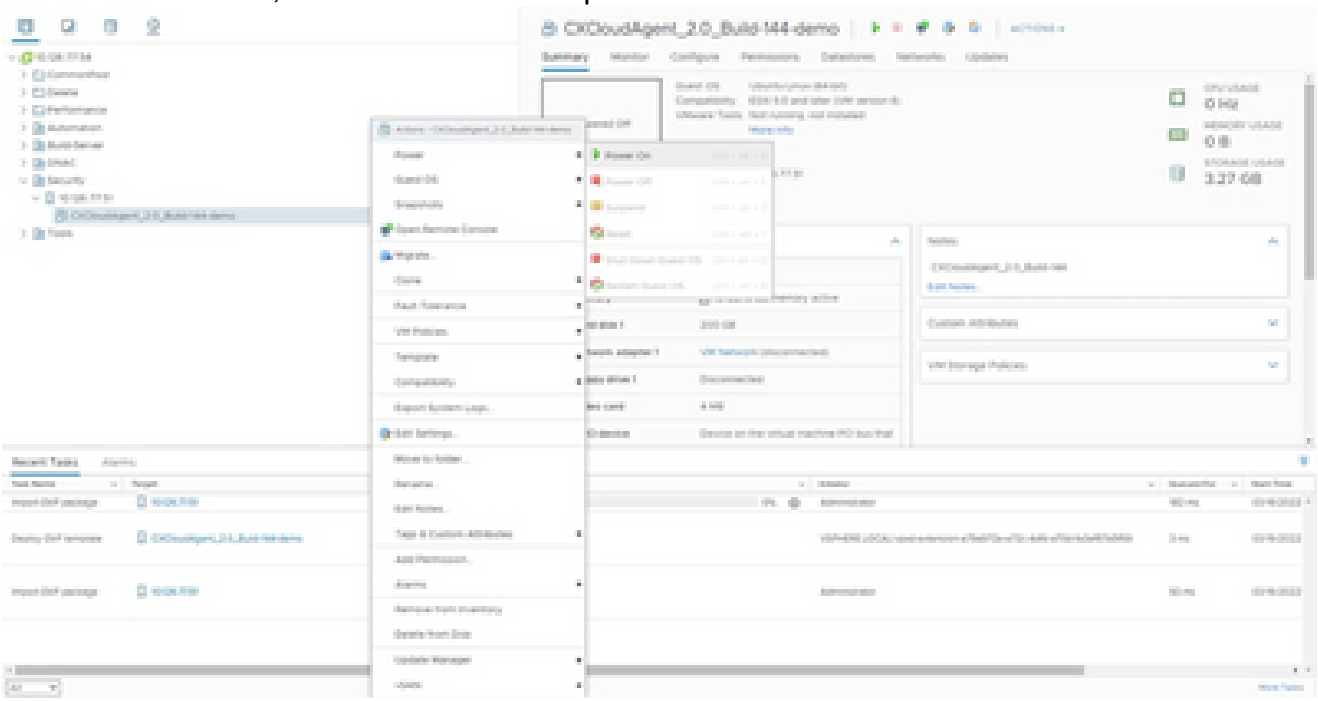
Pronto per il completamento

12. Fare clic sul nome della VM appena aggiunta per visualizzare lo stato.



VM aggiunta

13. Una volta installata, accendere la VM e aprire la console.



Apertura della console

14. Passare a Configurazione di rete per continuare con i passaggi successivi.

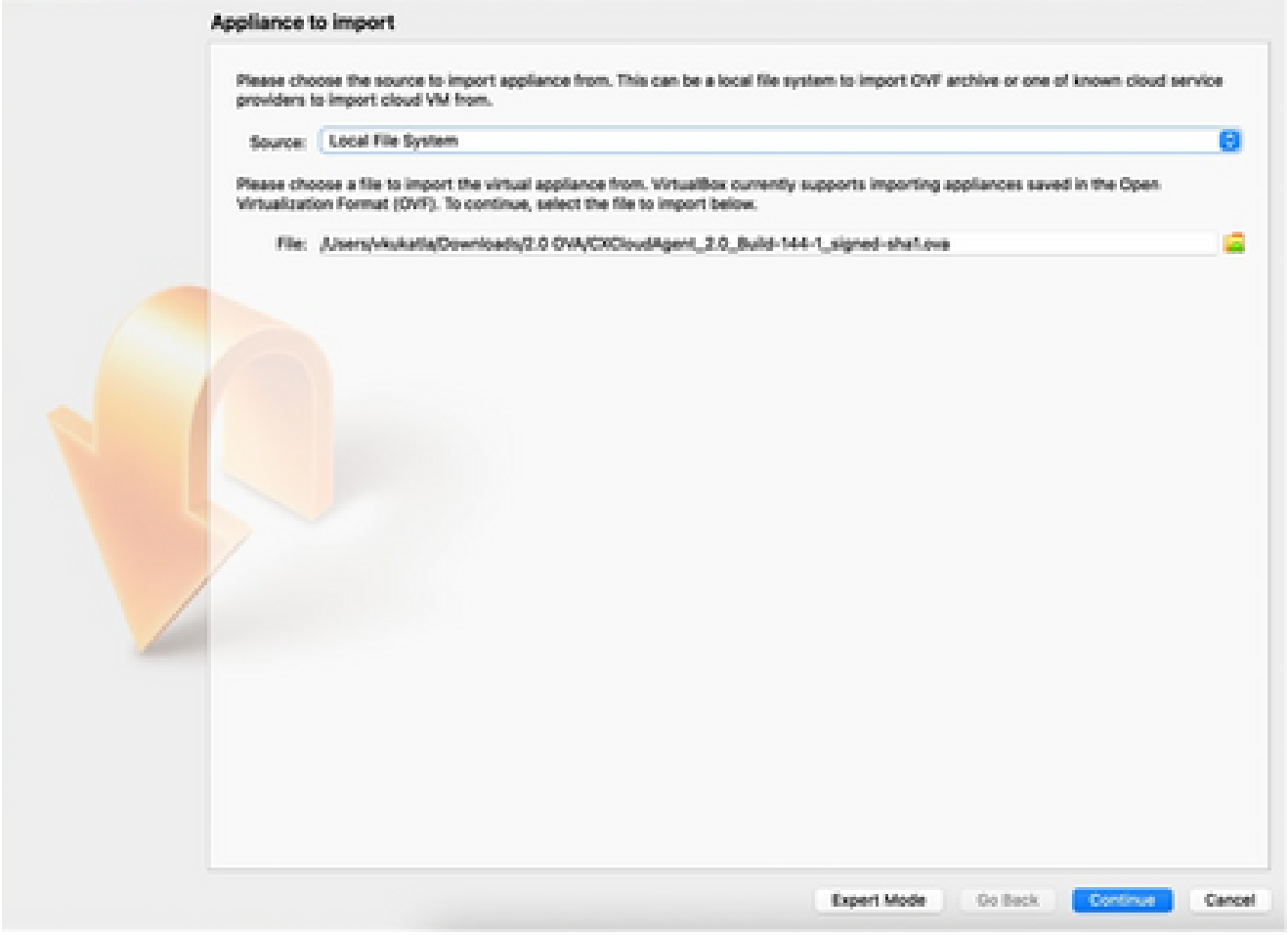
Installazione di Oracle Virtual Box 5.2.30

Questo client distribuisce l'OAV dell'agente cloud CX tramite Oracle Virtual Box.

1. Aprire l'interfaccia utente di Oracle VM e selezionare File> Importa accessorio.

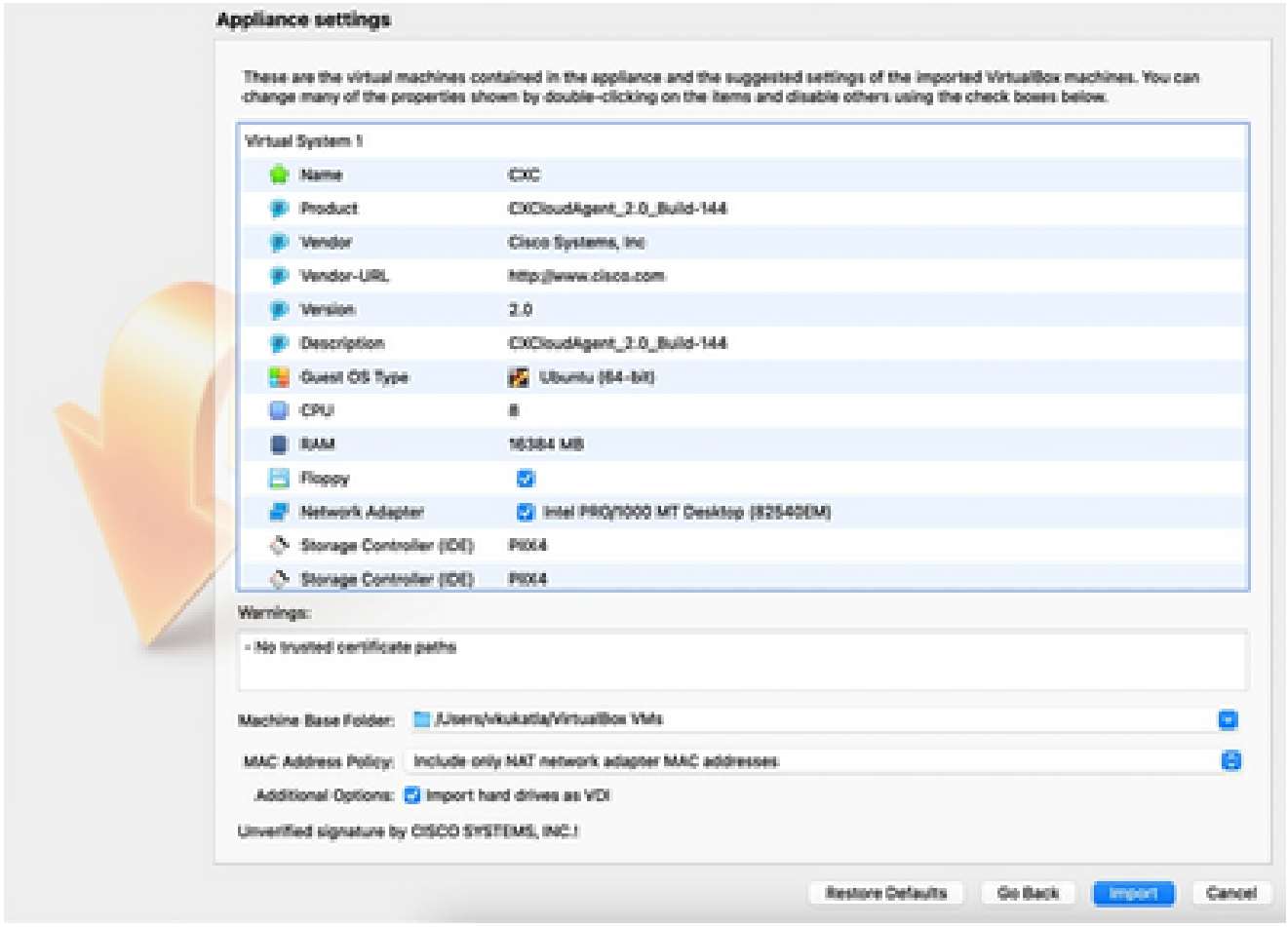
Oracle VM

2. Individuare il file OVA e importarlo.



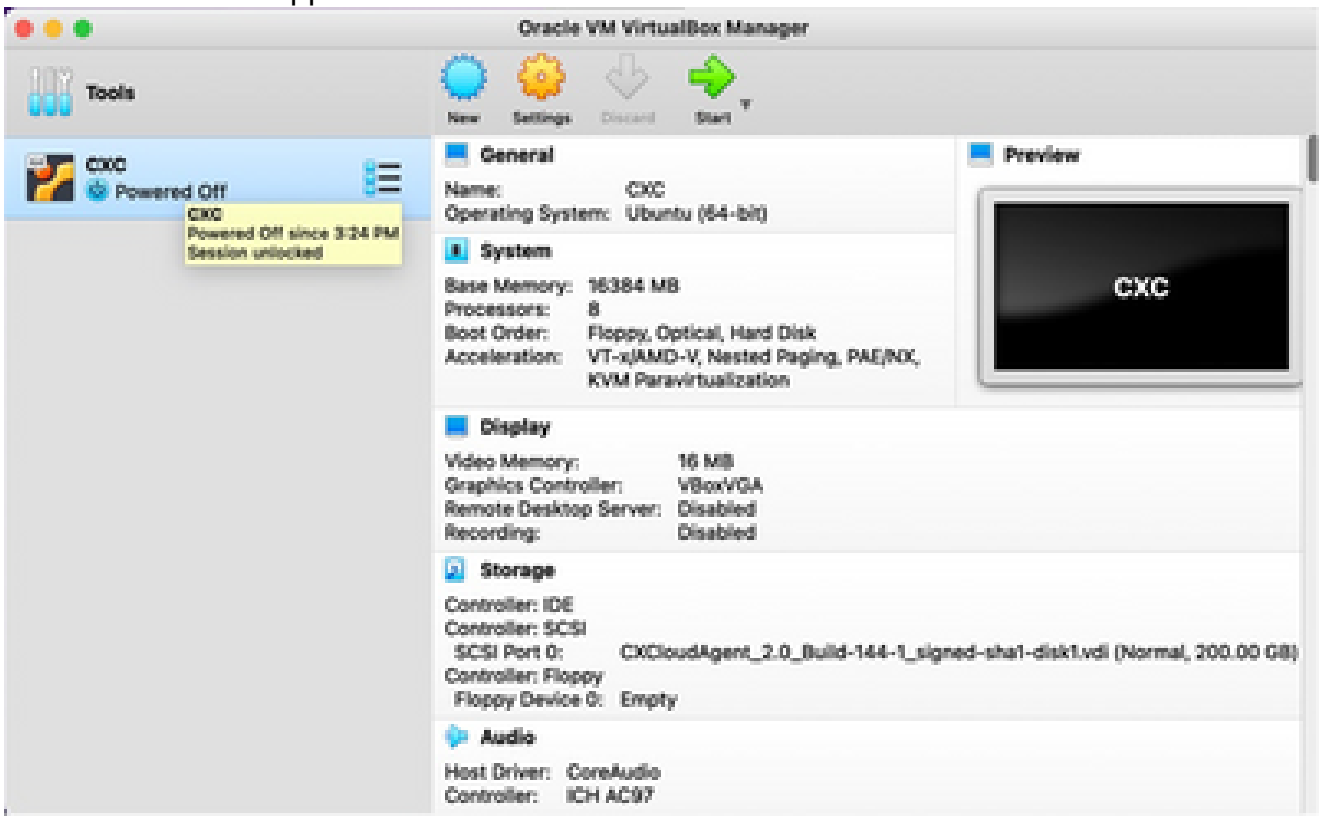
Selezione del file

3. Fare clic su Import (Importa).

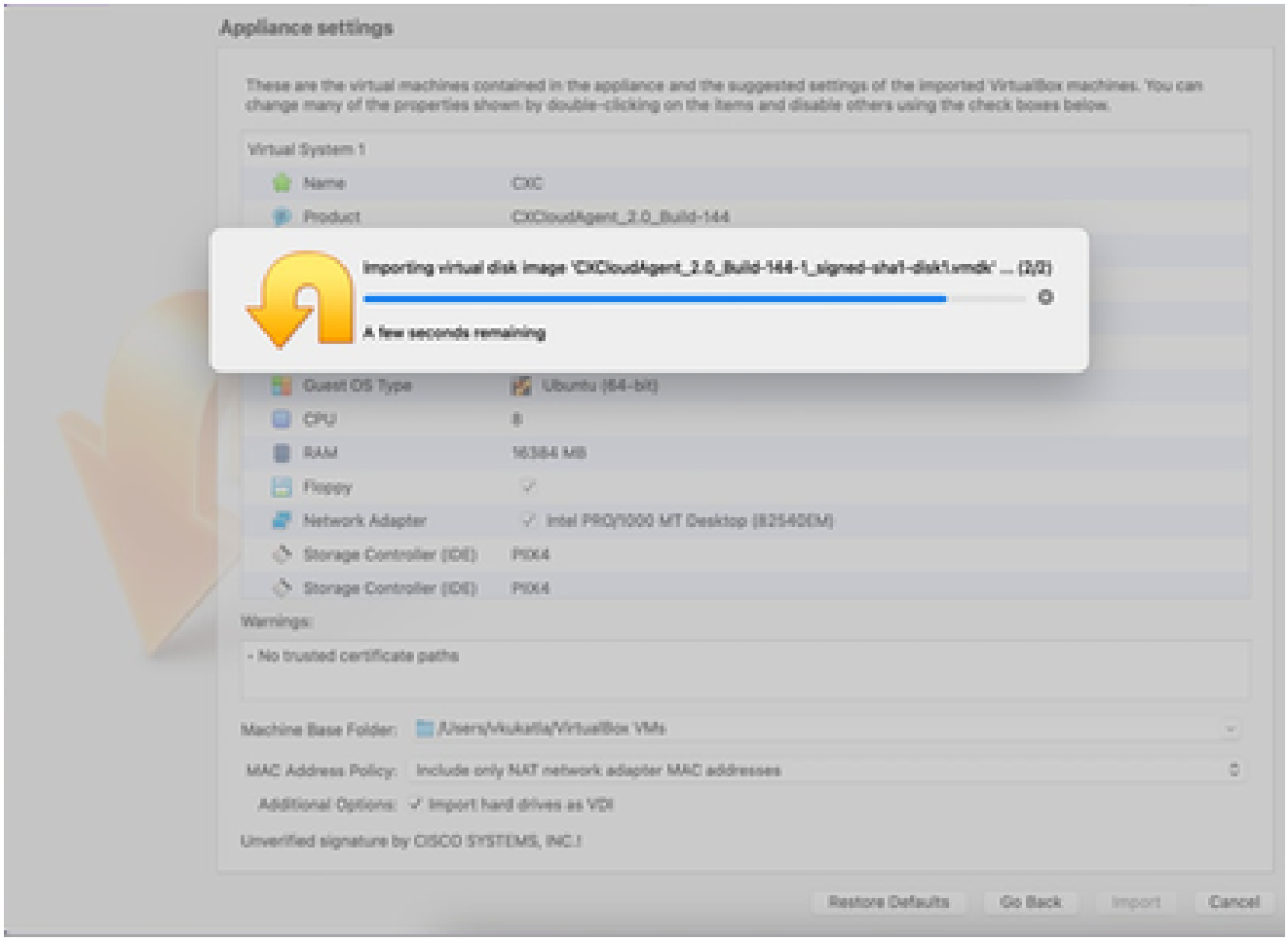


Importazione del file

4. Selezionare la VM appena distribuita e fare clic su Avvia.

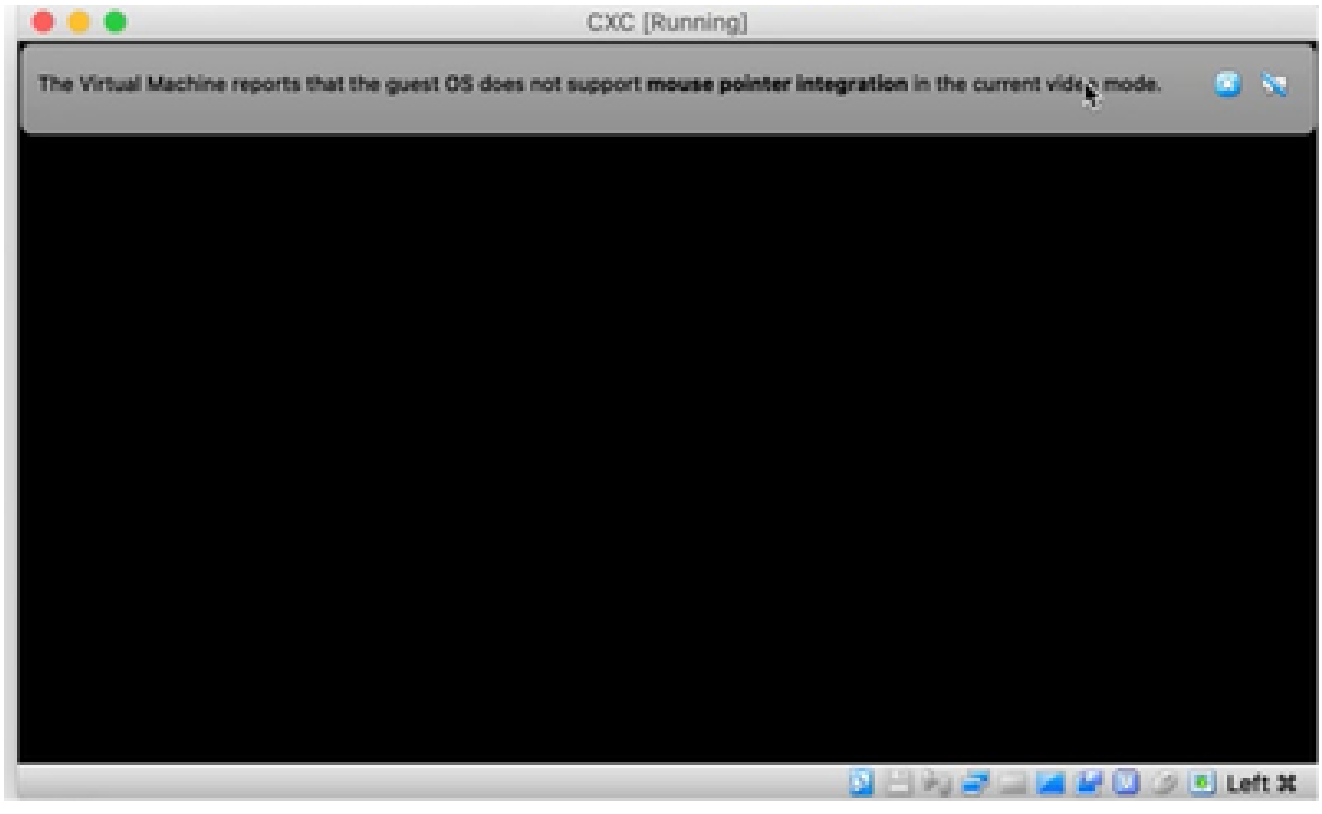


Avvio della console VM



Importazione in corso

5. Accendere la VM. Sulla console viene visualizzato.



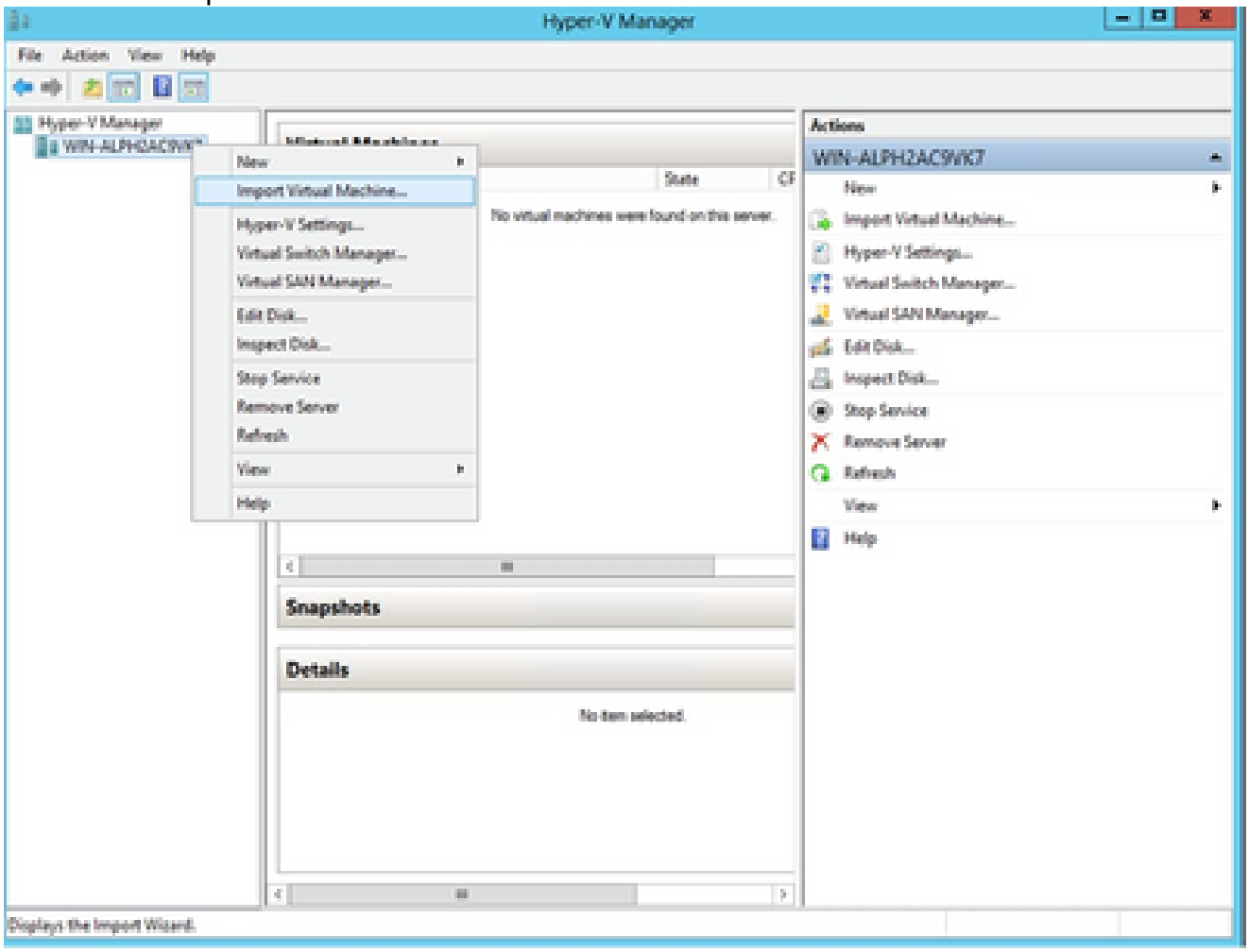
Apertura della console

6. Passare a Configurazione di rete per continuare con i passaggi successivi.

Installazione di Microsoft Hyper-V

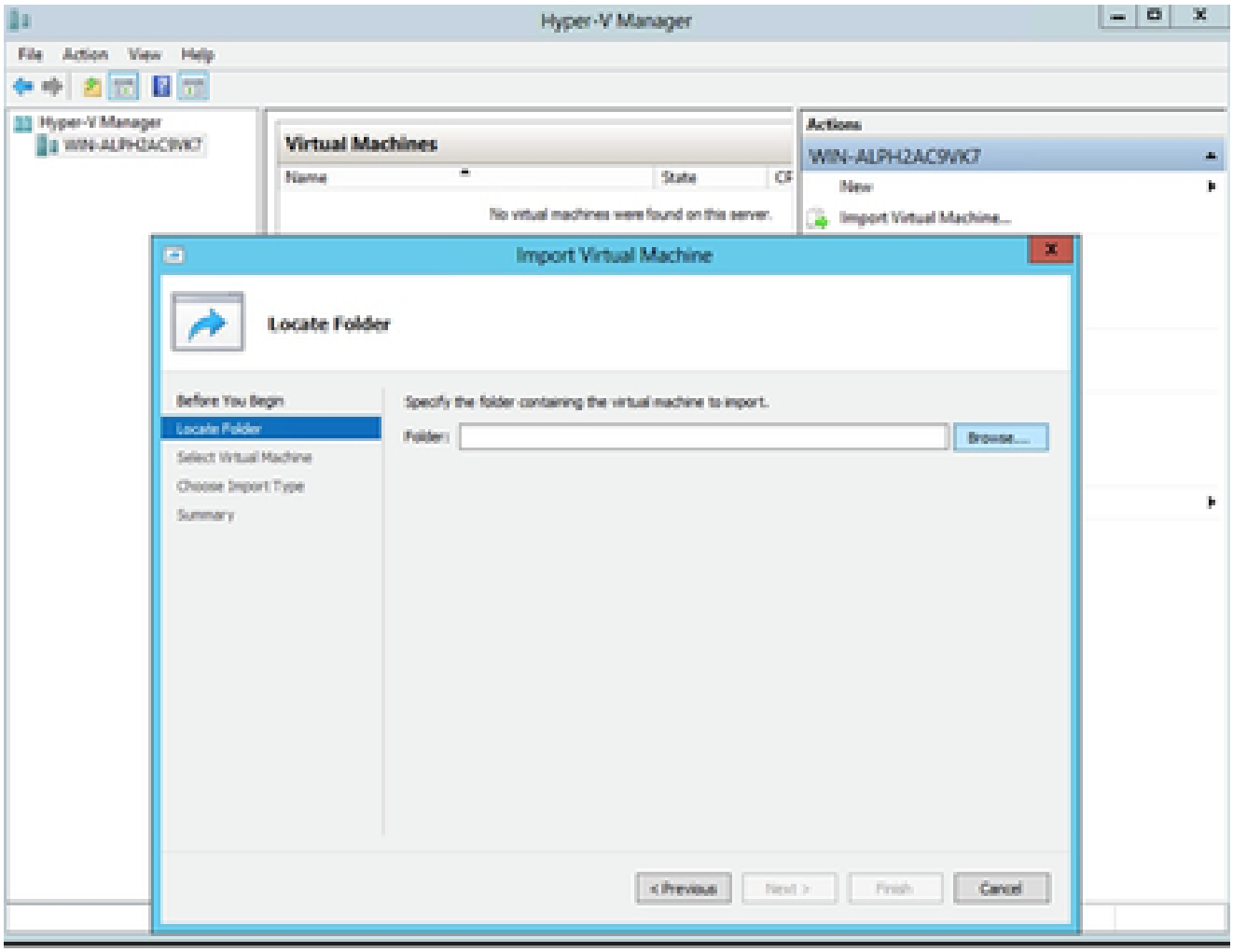
Eseguire questa procedura:

1. Selezionare Importa macchina virtuale.



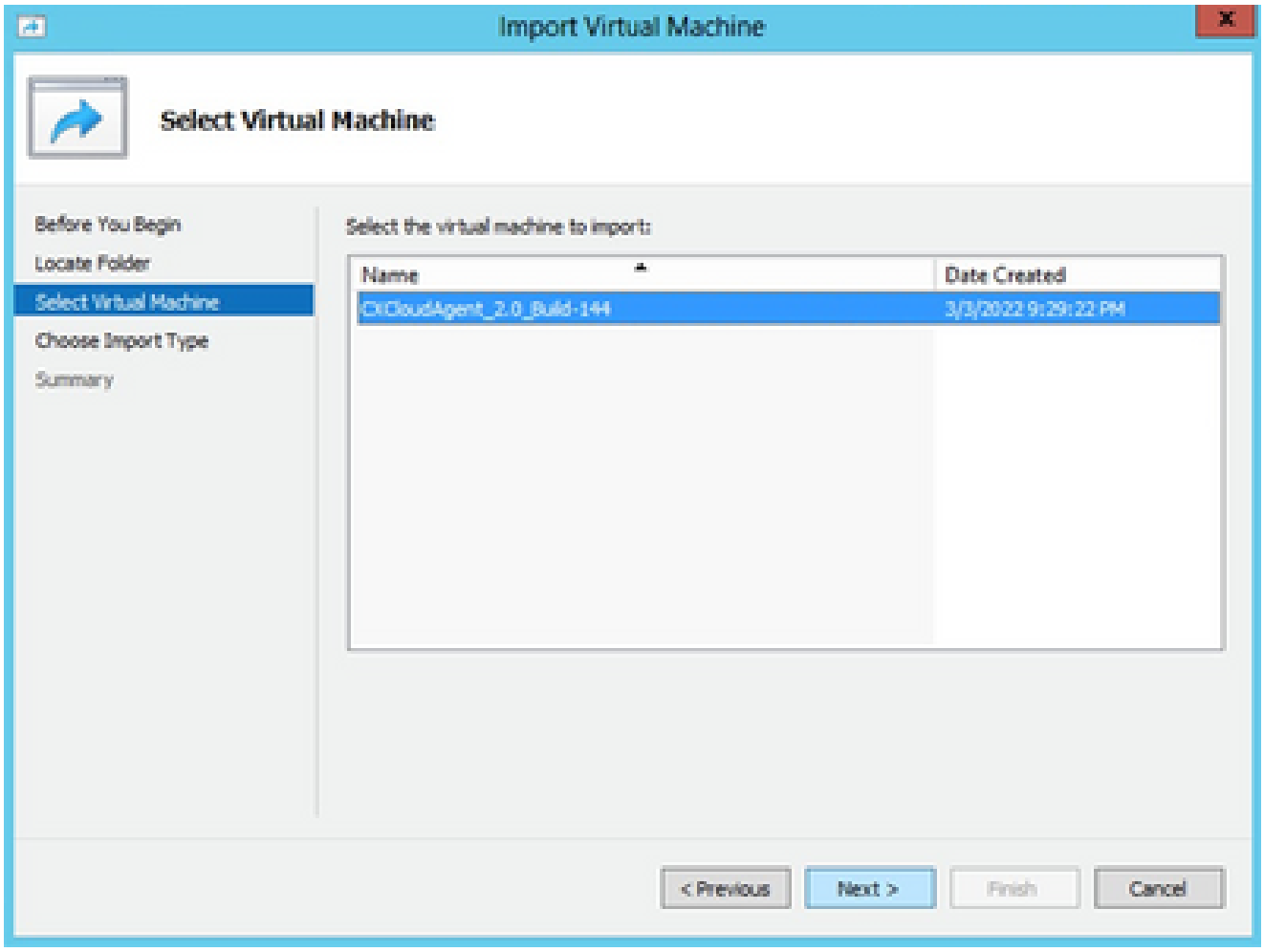
Gestione Hyper-V

2. Individuare la cartella di download e selezionarla.
3. Fare clic su Next (Avanti).



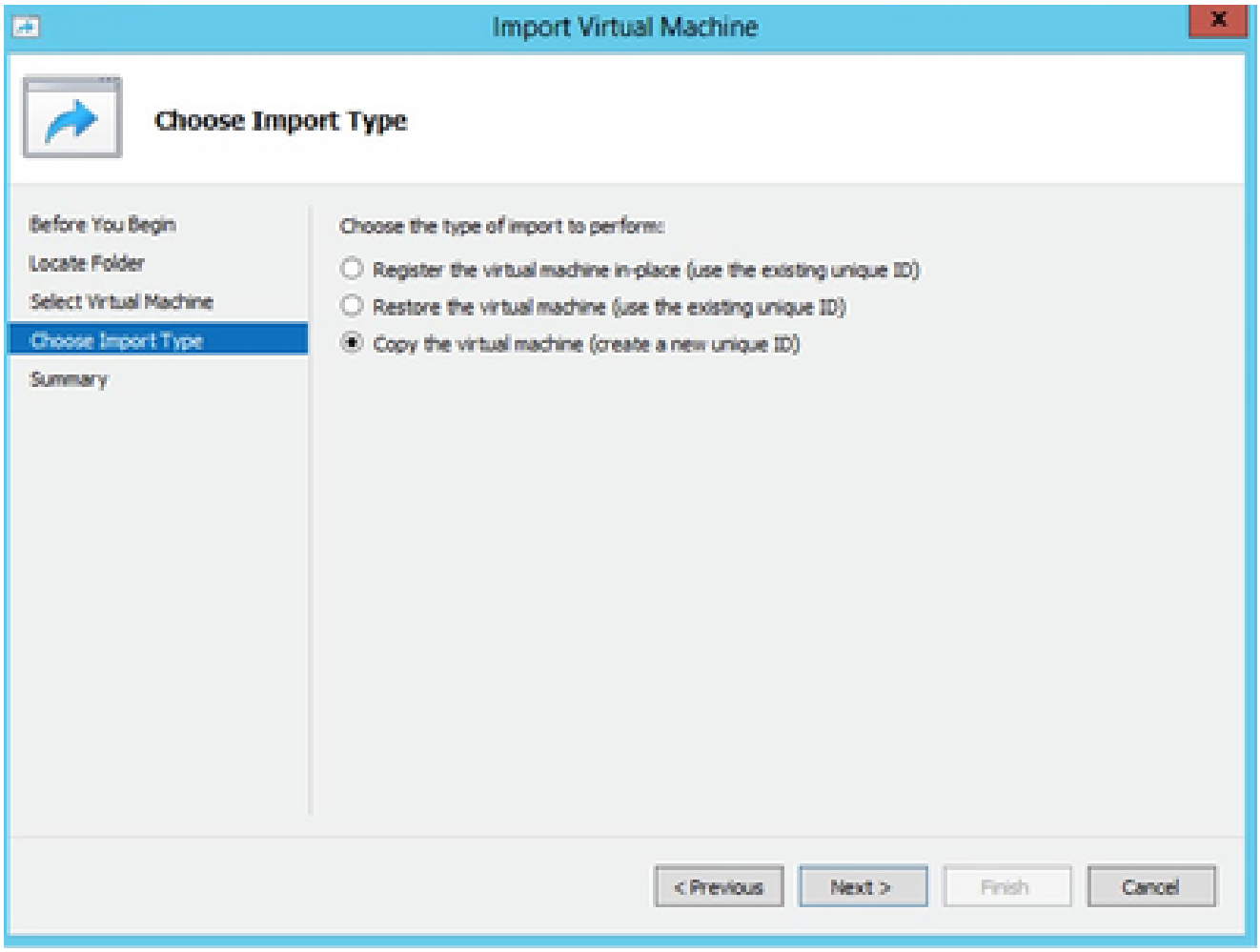
Cartella per l'importazione

4. Selezionare la VM e fare clic su Avanti.



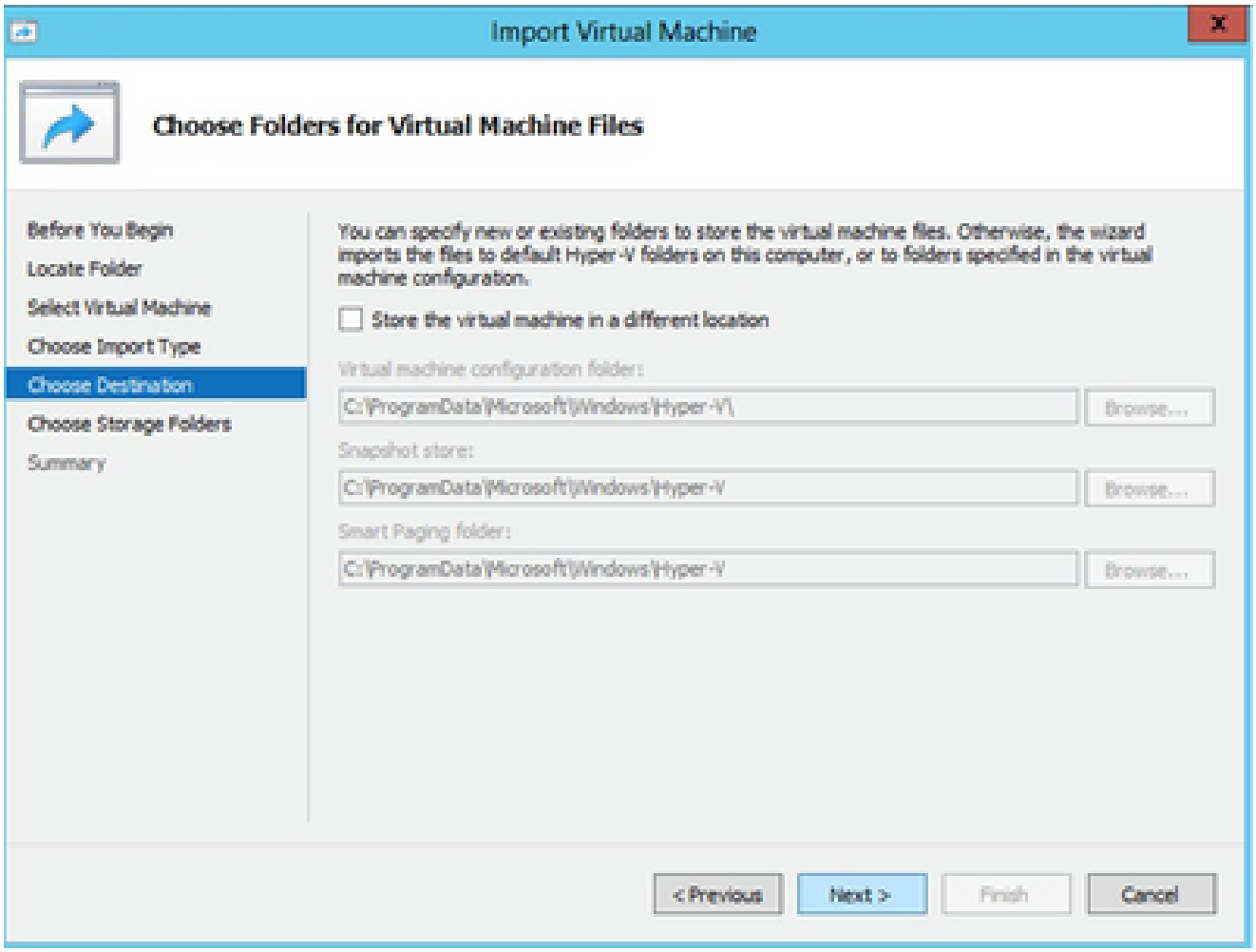
Selezione della VM

5. Selezionare il pulsante di opzione Copia la macchina virtuale (crea un nuovo ID univoco) e fare clic su Avanti.



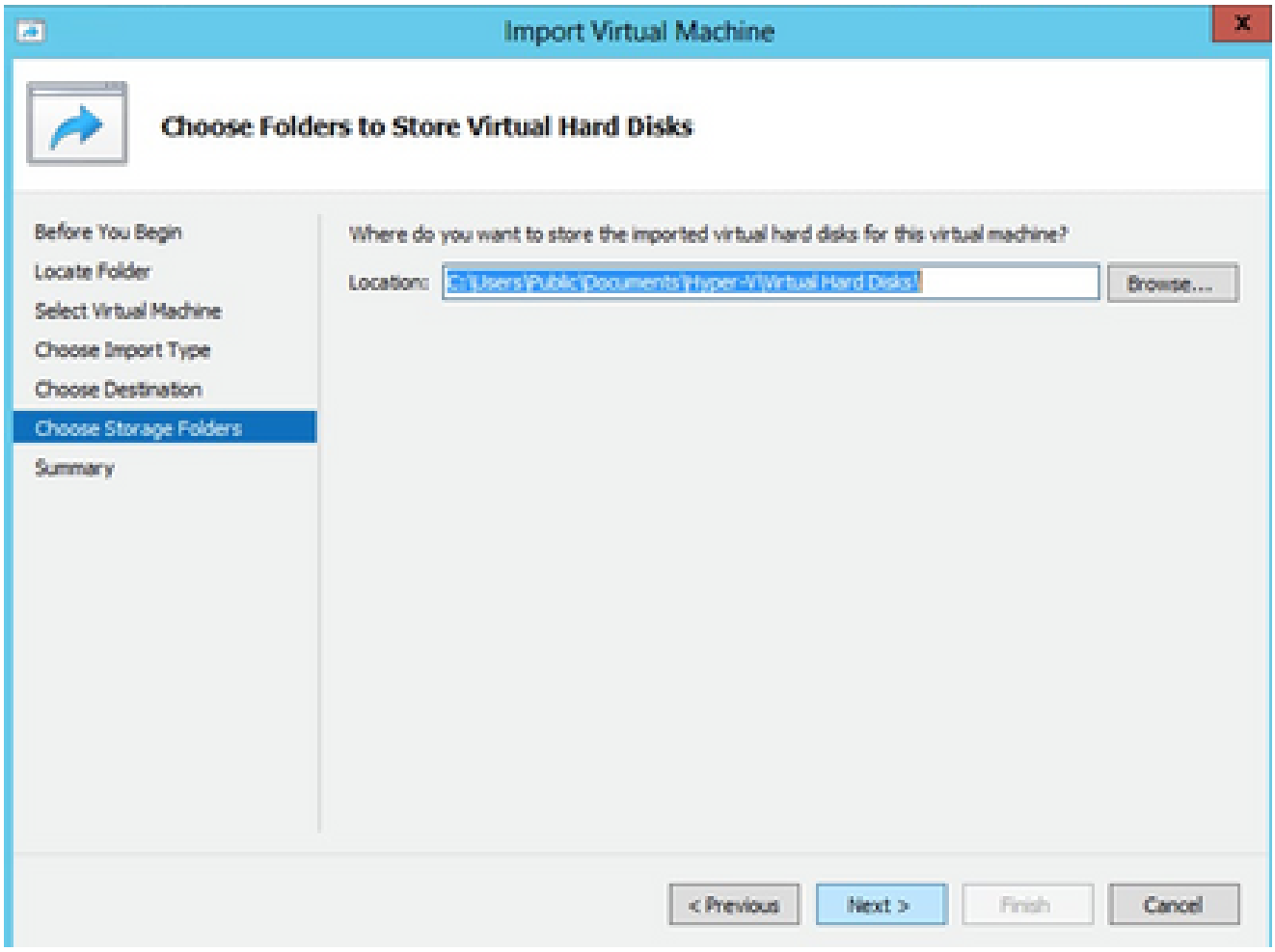
Tipo di importazione

6. Individuare la cartella dei file VM e selezionarla Si consiglia di utilizzare i percorsi predefiniti.
7. Fare clic su Next (Avanti).



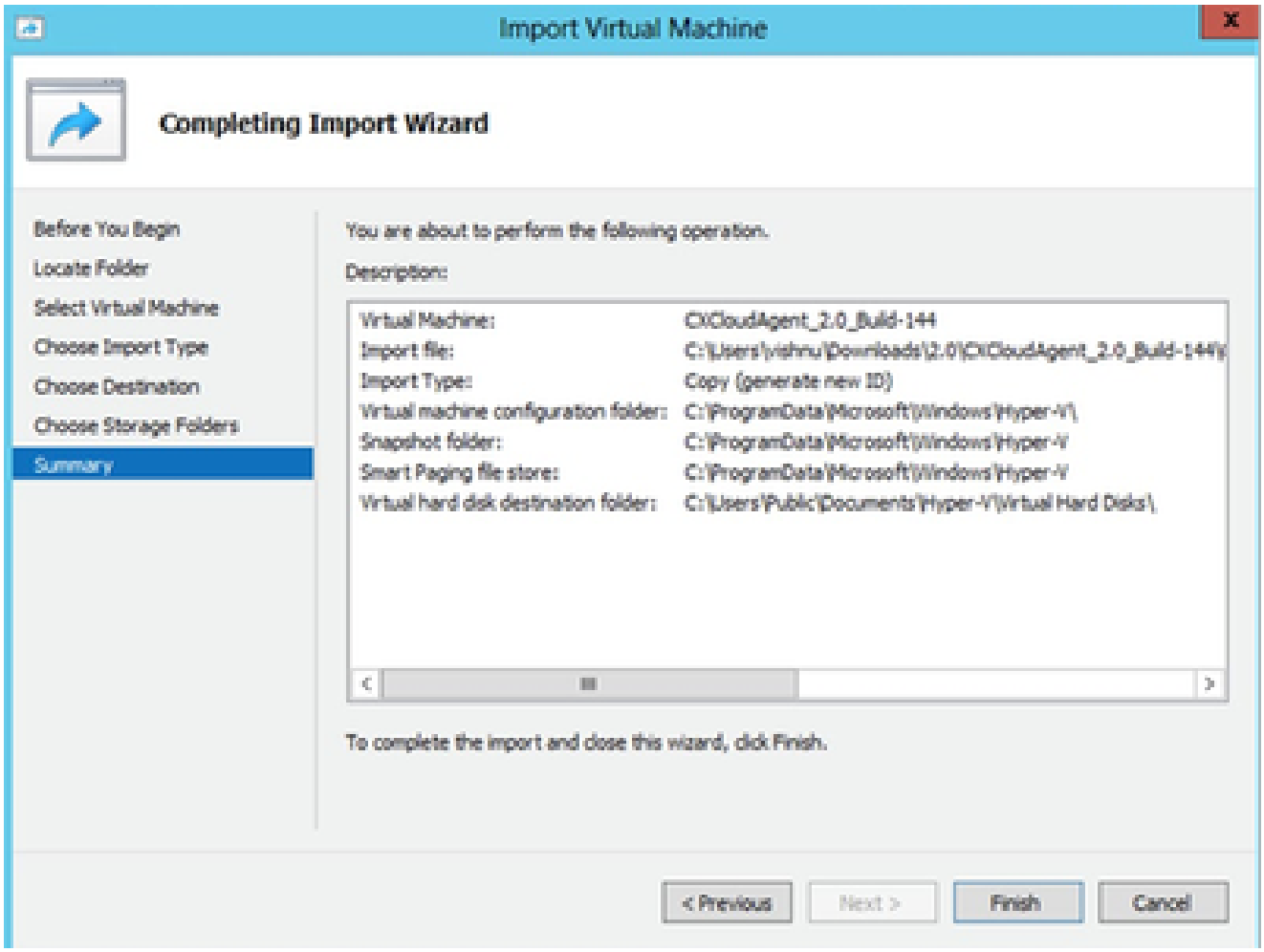
Scegliere le cartelle per i file delle macchine virtuali

8. Individuare la cartella in cui archiviare il disco rigido della VM Si consiglia di utilizzare i percorsi predefiniti.
9. Fare clic su Next (Avanti).



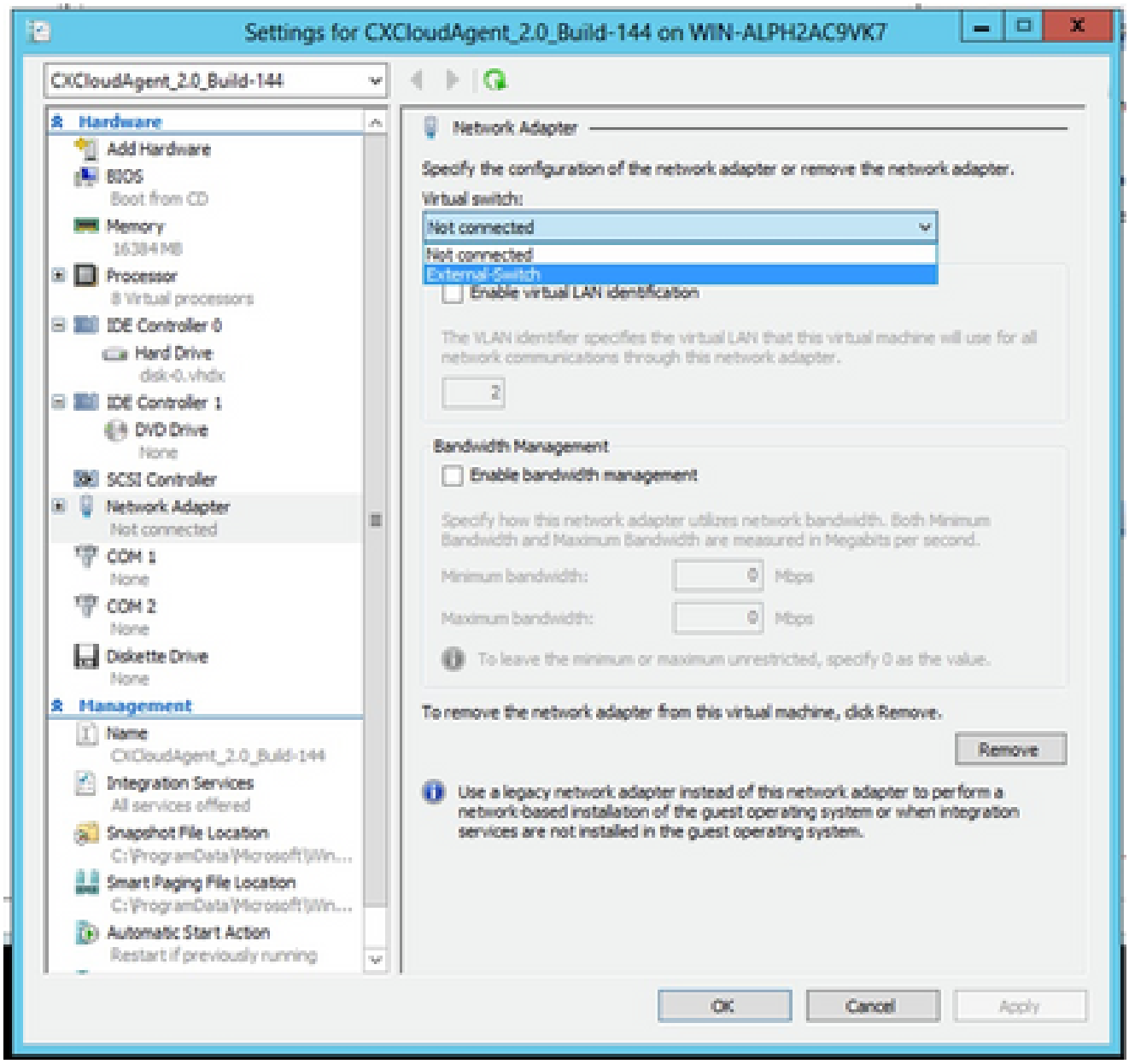
Cartella per l'archiviazione dei dischi rigidi virtuali

10. Viene visualizzato il riepilogo della VM. Verificare tutti gli input e fare clic su Fine.



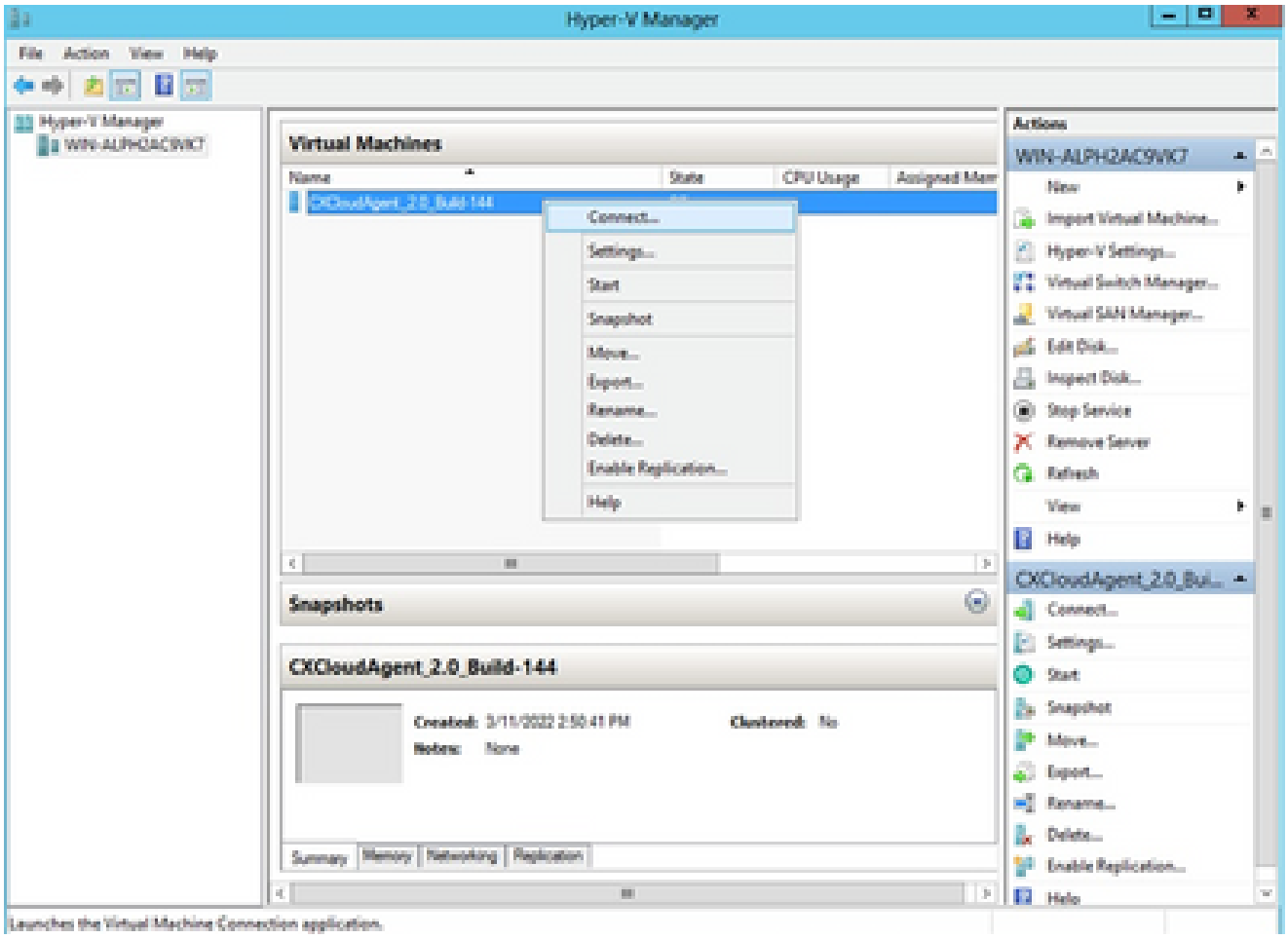
Riepilogo

11. Al termine dell'importazione, viene creata una nuova VM in Hyper-V. Aprire l'impostazione della VM.
12. Selezionare la scheda di rete sul riquadro a sinistra e selezionare Virtual Switch (Switch virtuale) dall'elenco a discesa.



Switch virtuale

13. Selezionare Connect (Connetti) per avviare la VM.

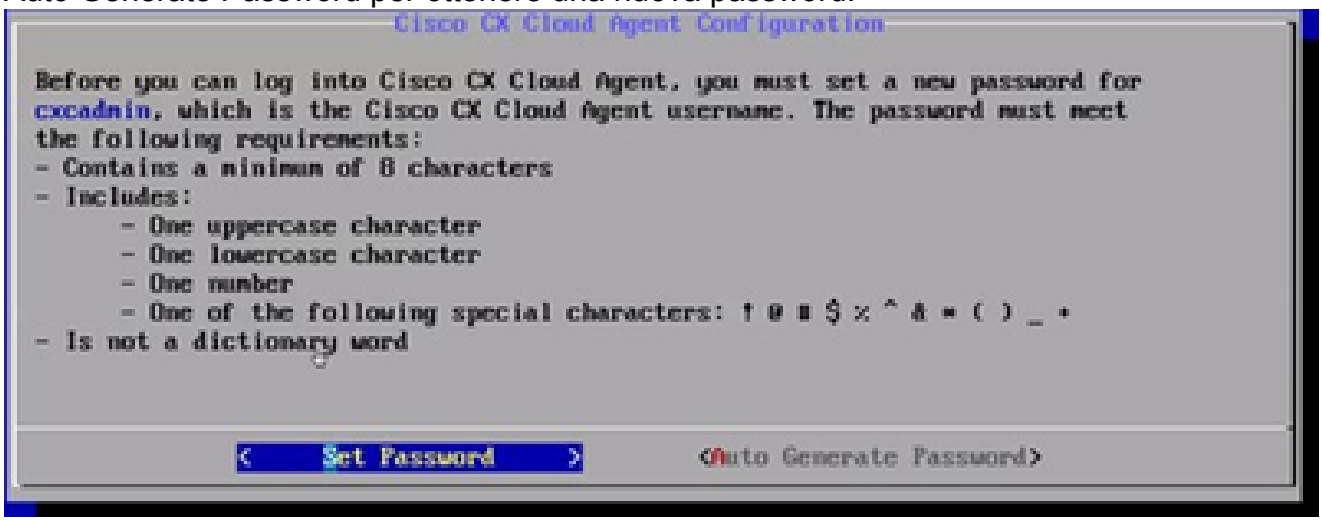


Avvio della VM

14. Passare a Configurazione di rete per continuare con i passaggi successivi.

Configurazione della rete

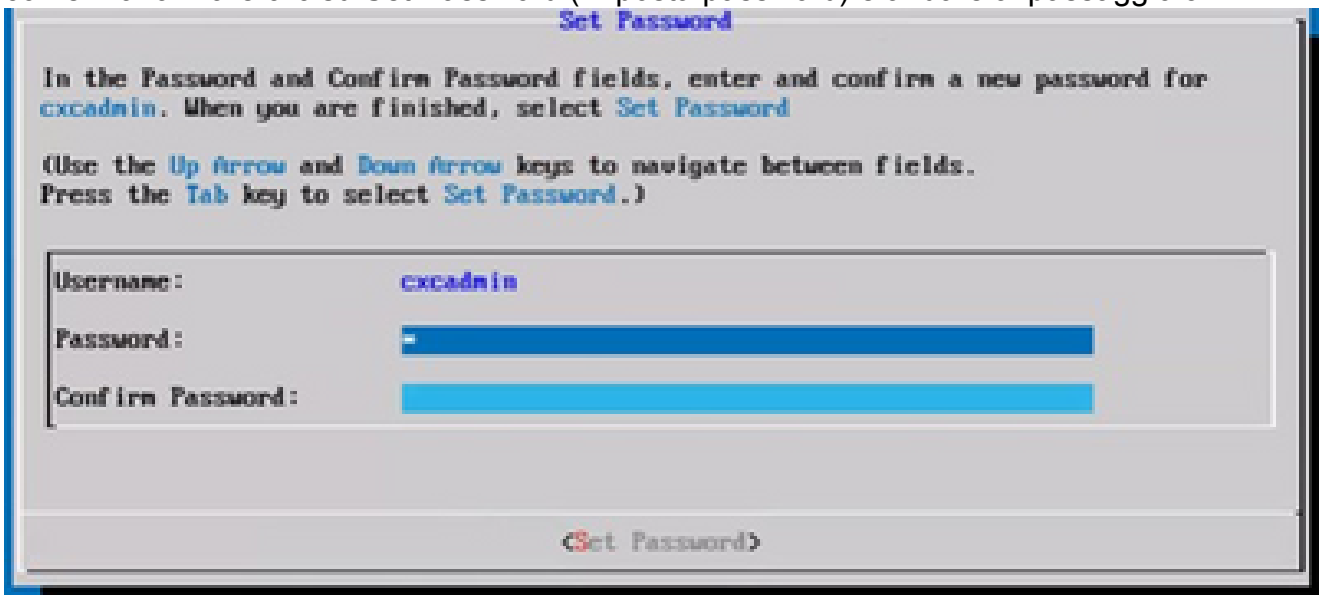
1. Fare clic su Set Password per aggiungere una nuova password per cxcadmin OPPURE su Auto Generate Password per ottenere una nuova password.



Imposta password

2. Se si seleziona Set Password (Imposta password), immettere la password per cxcadmin e

confermarla. Fare clic su Set Password (Imposta password) e andare al passaggio 3.



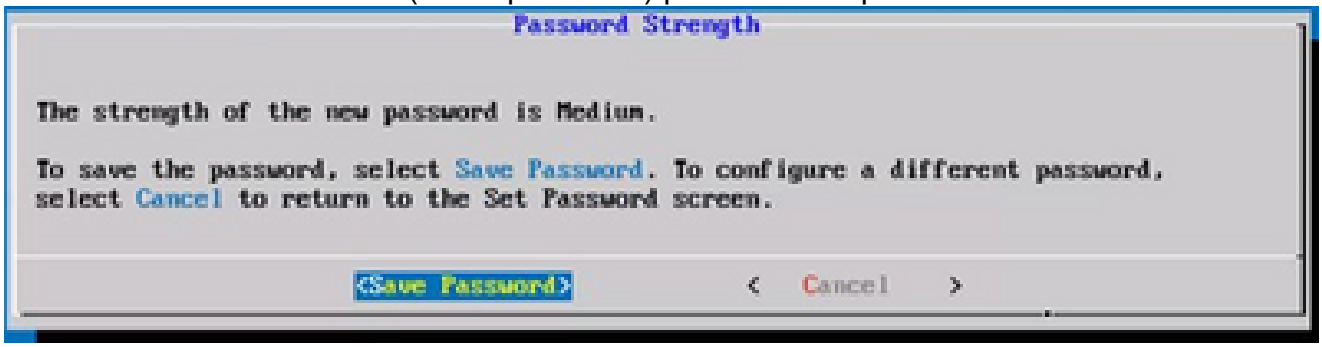
Nuova password

O

Se è selezionata l'opzione Generazione automatica password, copiare la password generata e memorizzarla per utilizzarla in futuro. Fare clic su Save Password (Salva password) e andare al passaggio 4.

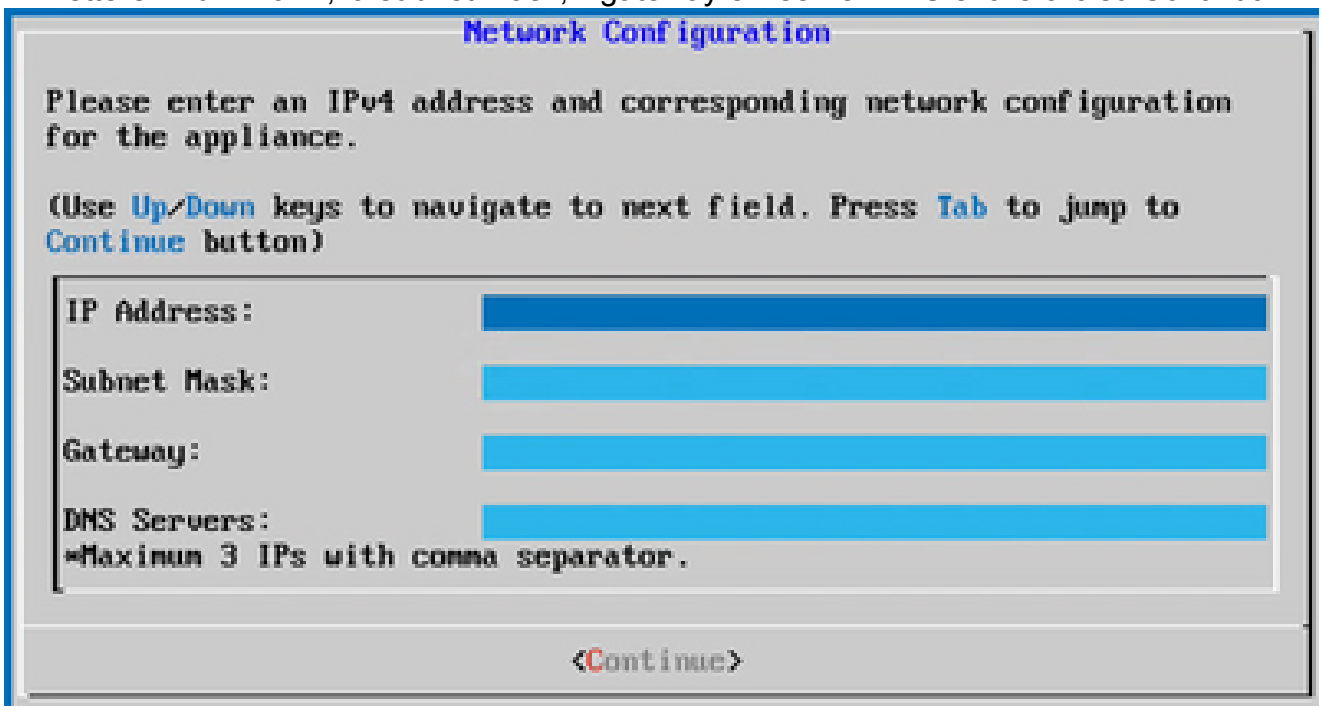
Password generata automaticamente

3. Fare clic su Save Password (Salva password) per utilizzarla per l'autenticazione.



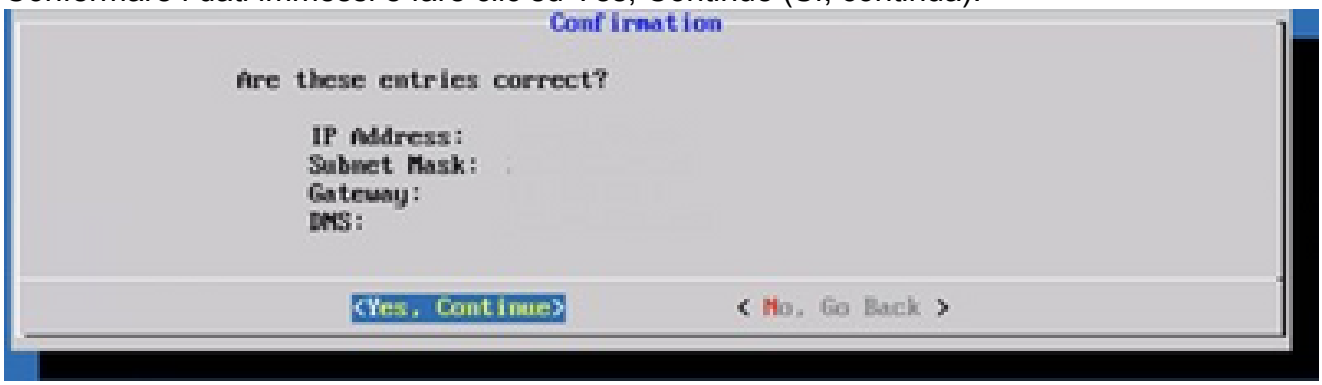
Salva password

4. Immettere l'indirizzo IP, la subnet mask, il gateway e il server DNS e fare clic su Continua.



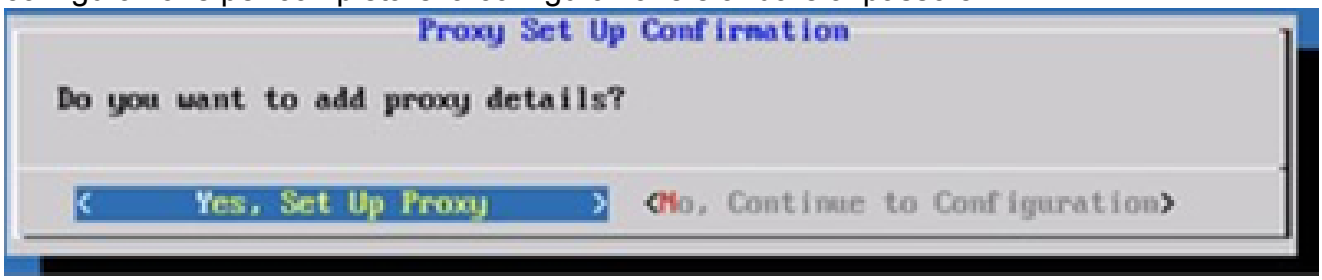
Configurazione della rete

5. Confermare i dati immessi e fare clic su Yes, Continue (Sì, continua).



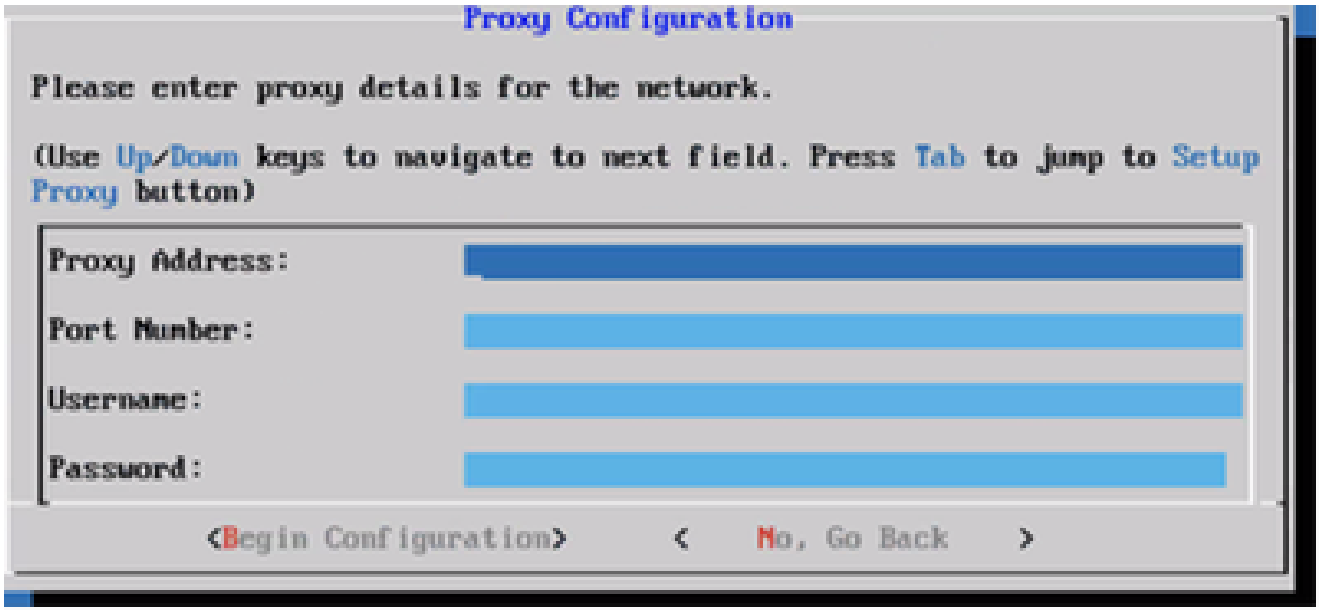
Configurazione

6. Per impostare i dettagli del proxy, fare clic su Sì, Configura proxy o su No, Continua con la configurazione per completare la configurazione e andare al passo 8.



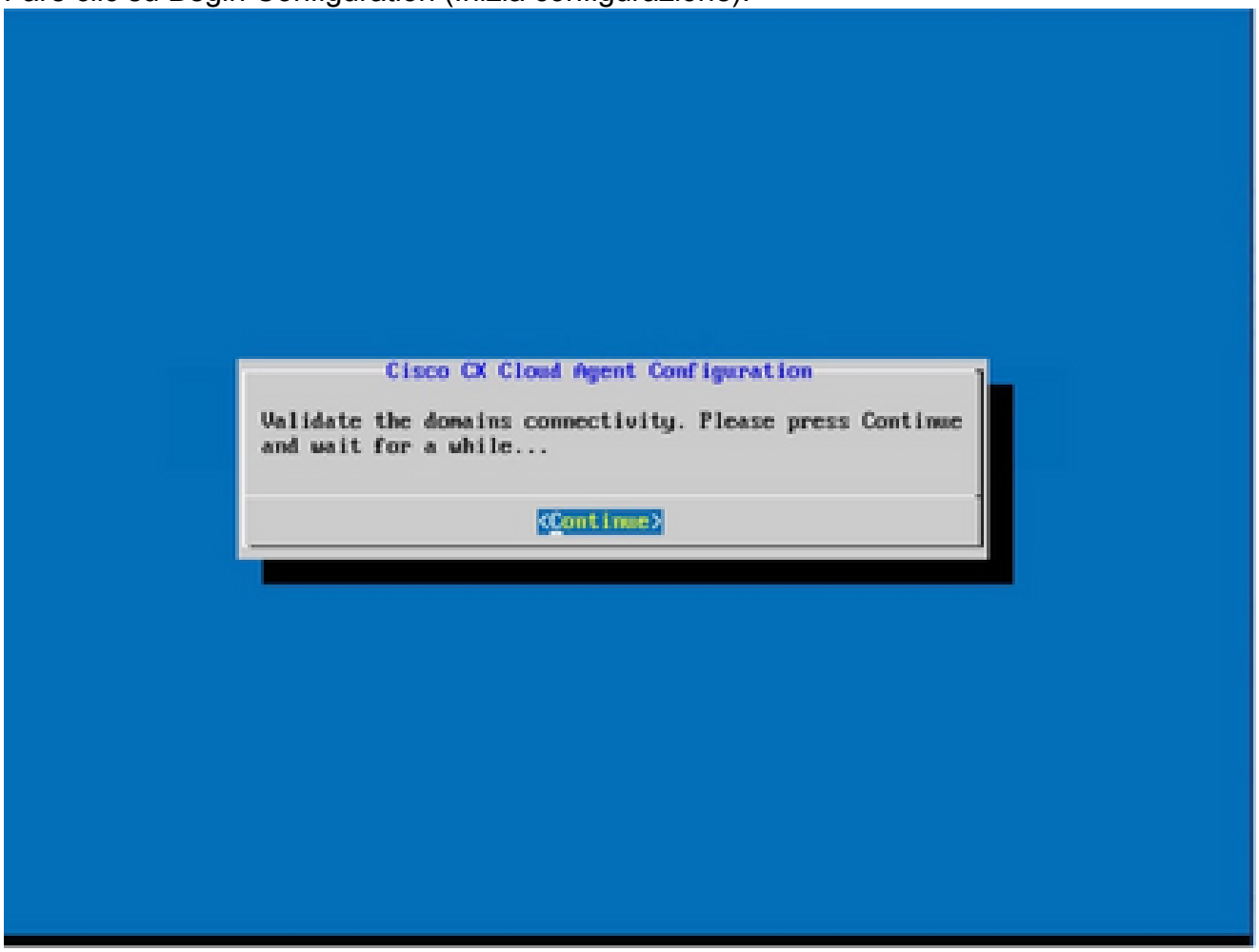
Impostazione del proxy

7. Immettere l'indirizzo proxy, il numero di porta, il nome utente e la password.



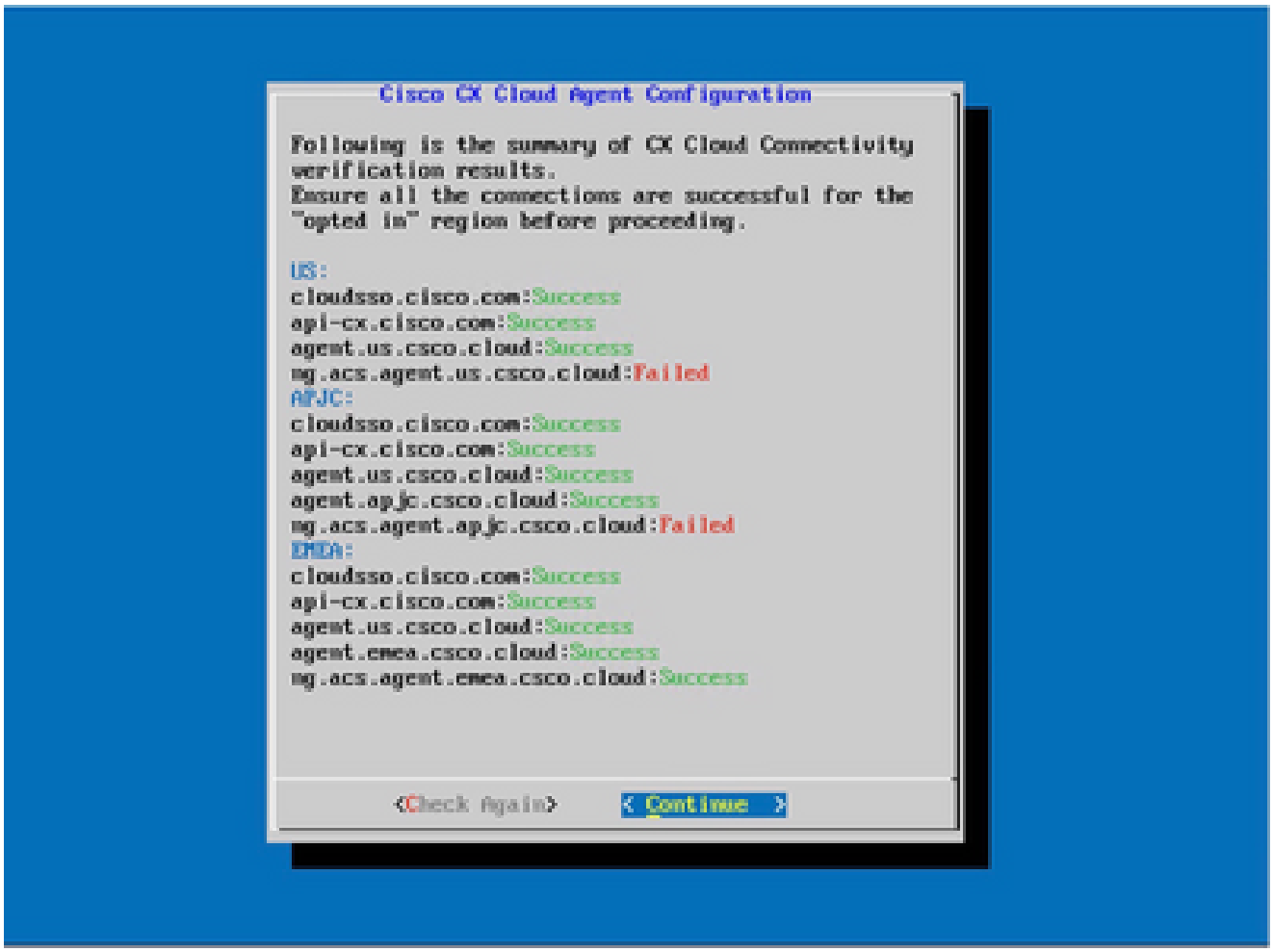
Configurazione del proxy

8. Fare clic su Begin Configuration (Inizia configurazione).



Inizio configurazione

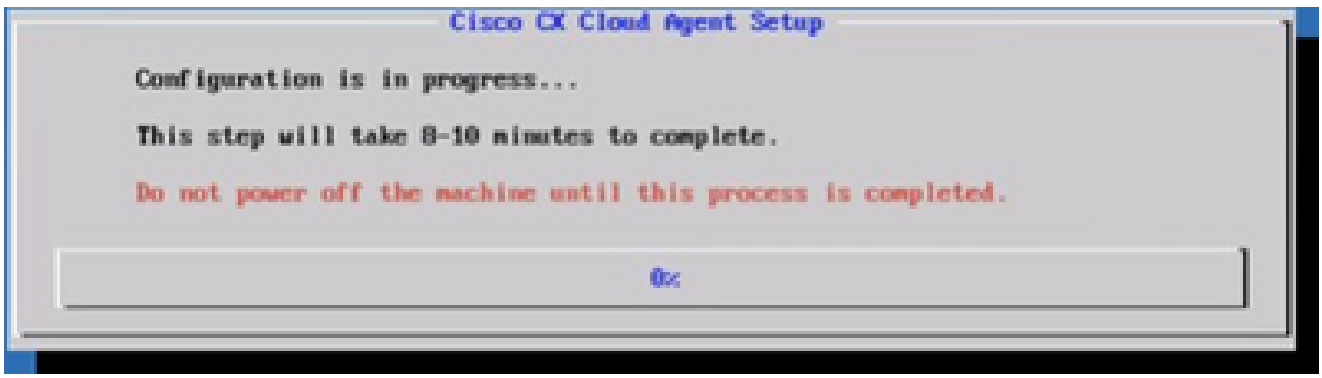
9. Fare clic su Continue (Continua).



Configurazione continua

10. Fare clic su Continue (Continua) per procedere con la configurazione in modo che il dominio raggiunga correttamente il dominio. Il completamento della configurazione può richiedere alcuni minuti.

Nota: se i domini non possono essere raggiunti correttamente, il cliente deve correggere la raggiungibilità del dominio apportando modifiche nel firewall per assicurare che i domini siano raggiungibili. Fare clic su Controlla di nuovo dopo aver risolto il problema di raggiungibilità dei domini.

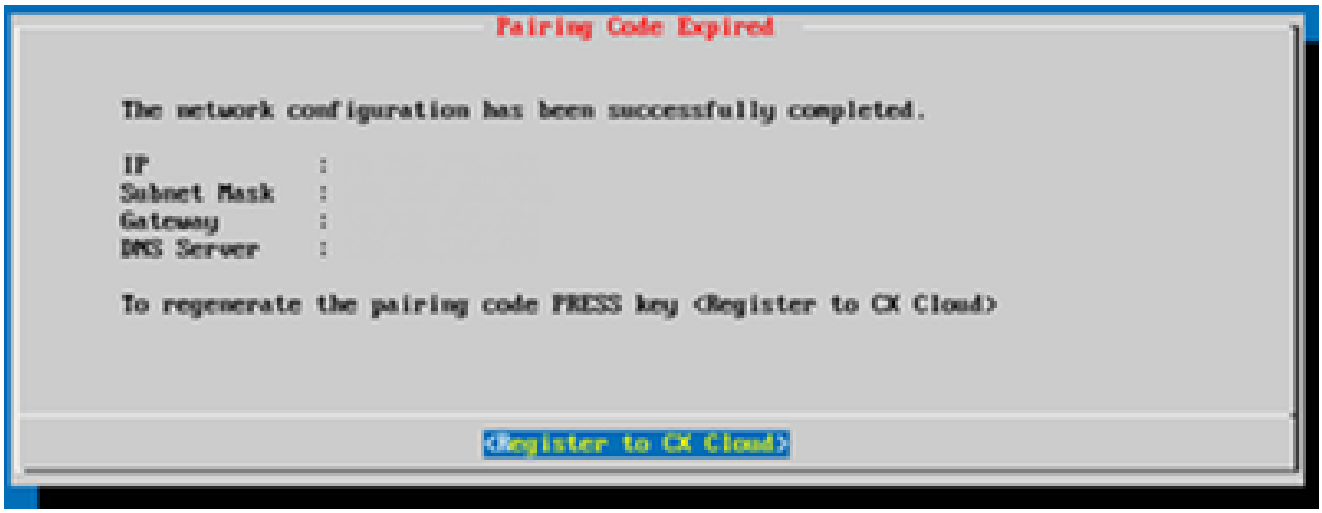


Configurazione in corso

11. Copiare il codice di associazione e tornare a CX Cloud per proseguire.

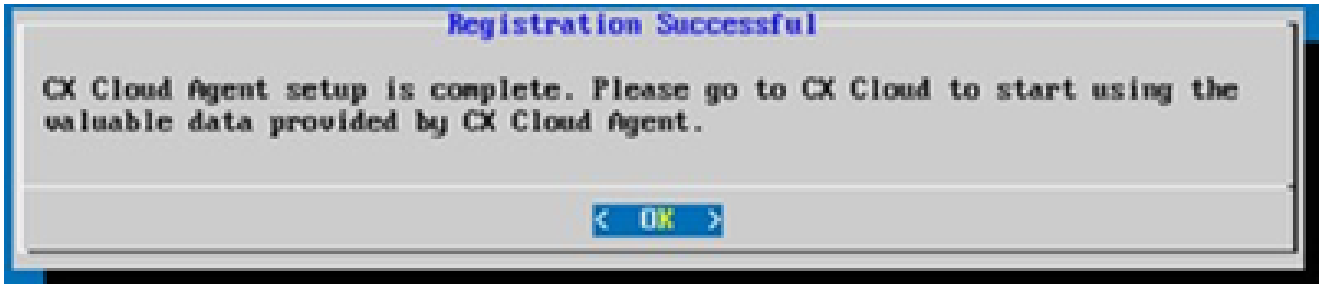
Codice di associazione

12. Se il codice di associazione scade, fare clic su Register to CX Cloud per ottenere di nuovo il codice.



Codice scaduto

13. Fare clic su OK.



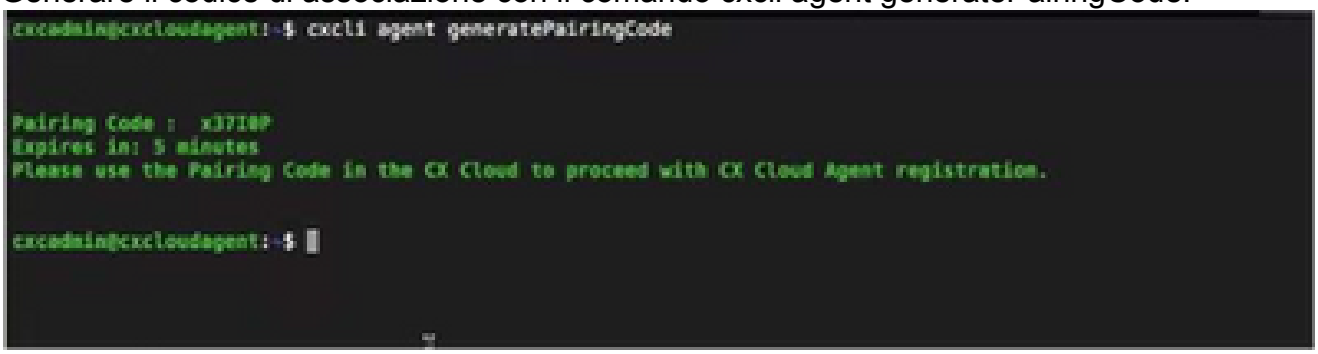
Registrazione completata

Approccio alternativo per generare il codice di accoppiamento tramite CLI

Gli utenti possono anche generare un codice di associazione utilizzando le opzioni CLI.

Per generare un codice di associazione utilizzando CLI:

1. Accedere all'agente cloud tramite SSH utilizzando le credenziali utente cxcadmin.
2. Generare il codice di associazione con il comando cxcli agent generatePairingCode.



Generazione del codice di associazione dalla CLI

3. Copiare il codice di associazione e tornare a CX Cloud per proseguire.

Configurazione di Cisco DNA Center per l'inoltro del syslog all'agente cloud CX

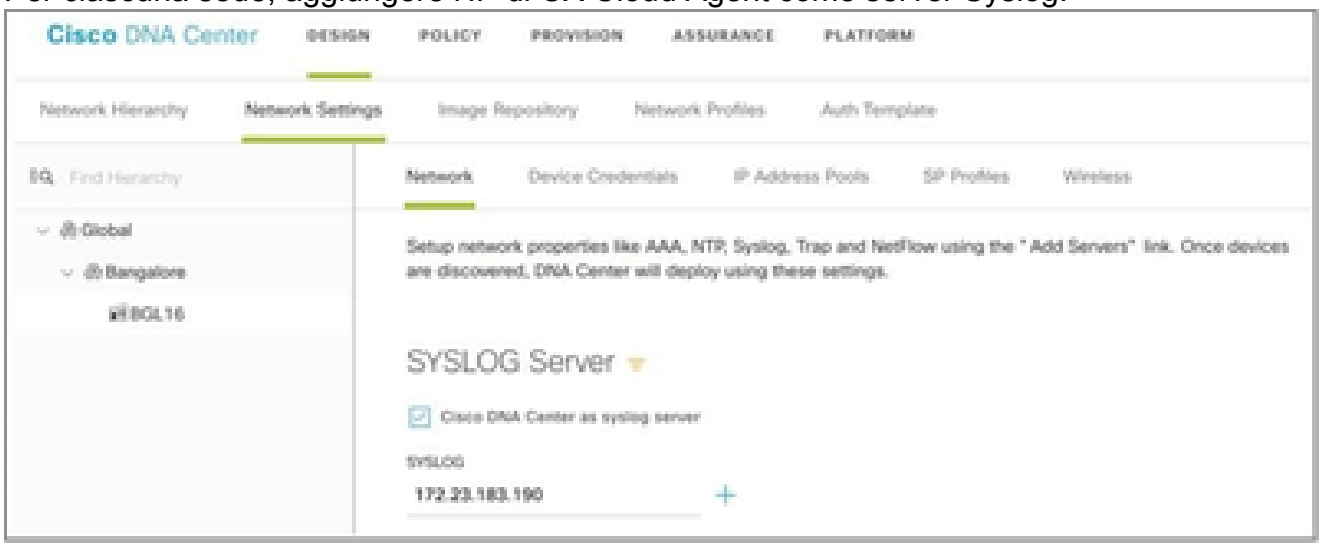
Prerequisiti

Le versioni supportate di Cisco DNA Center sono dalla 2.1.2.0 alla 2.2.3.5, dalla 2.3.3.4 alla 2.3.3.6, dalla 2.3.5.0 e da Cisco DNA Center Virtual Appliance

Configura impostazione inoltro syslog

Per configurare l'inoltro Syslog all'agente cloud CX nel Cisco DNA Center, attenersi alla seguente procedura:

1. Avviare Cisco DNA Center.
2. Andare a Design > Network Settings > Network (Progetto > Impostazioni di rete > Rete).
3. Per ciascuna sede, aggiungere l'IP di CX Cloud Agent come server Syslog.



Server Syslog

Note:
Una volta configurati, tutti i dispositivi associati a quel sito sono configurati per inviare syslog con il livello critico all'agente cloud CX. I dispositivi devono essere associati a un sito per abilitare l'inoltro syslog dal dispositivo all'agente cloud CX. Quando si aggiorna l'impostazione di un server syslog, tutti i dispositivi associati al sito vengono impostati automaticamente sul livello critico predefinito.

Configurazione di altre risorse per l'inoltro del syslog all'agente cloud CX

I dispositivi devono essere configurati in modo da inviare messaggi Syslog all'agente cloud CX per utilizzare la funzione Fault Management di CX Cloud.

Nota: solo i dispositivi Campus Success Track di livello 2 possono configurare altre risorse per l'inoltro del syslog.

Server Syslog esistenti con funzionalità di inoltro

Eseguire le istruzioni di configurazione per il software del server syslog e aggiungere l'indirizzo IP dell'agente cloud CX come nuova destinazione.

Nota: quando si inoltrano i syslog, assicurarsi che l'indirizzo IP di origine del messaggio syslog originale venga mantenuto.

Server Syslog esistenti senza funzionalità di inoltro O senza server Syslog

Configurare ciascun dispositivo in modo che invii i syslog direttamente all'indirizzo IP dell'agente del cloud CX. Per i passaggi di configurazione specifici, consultare la documentazione.

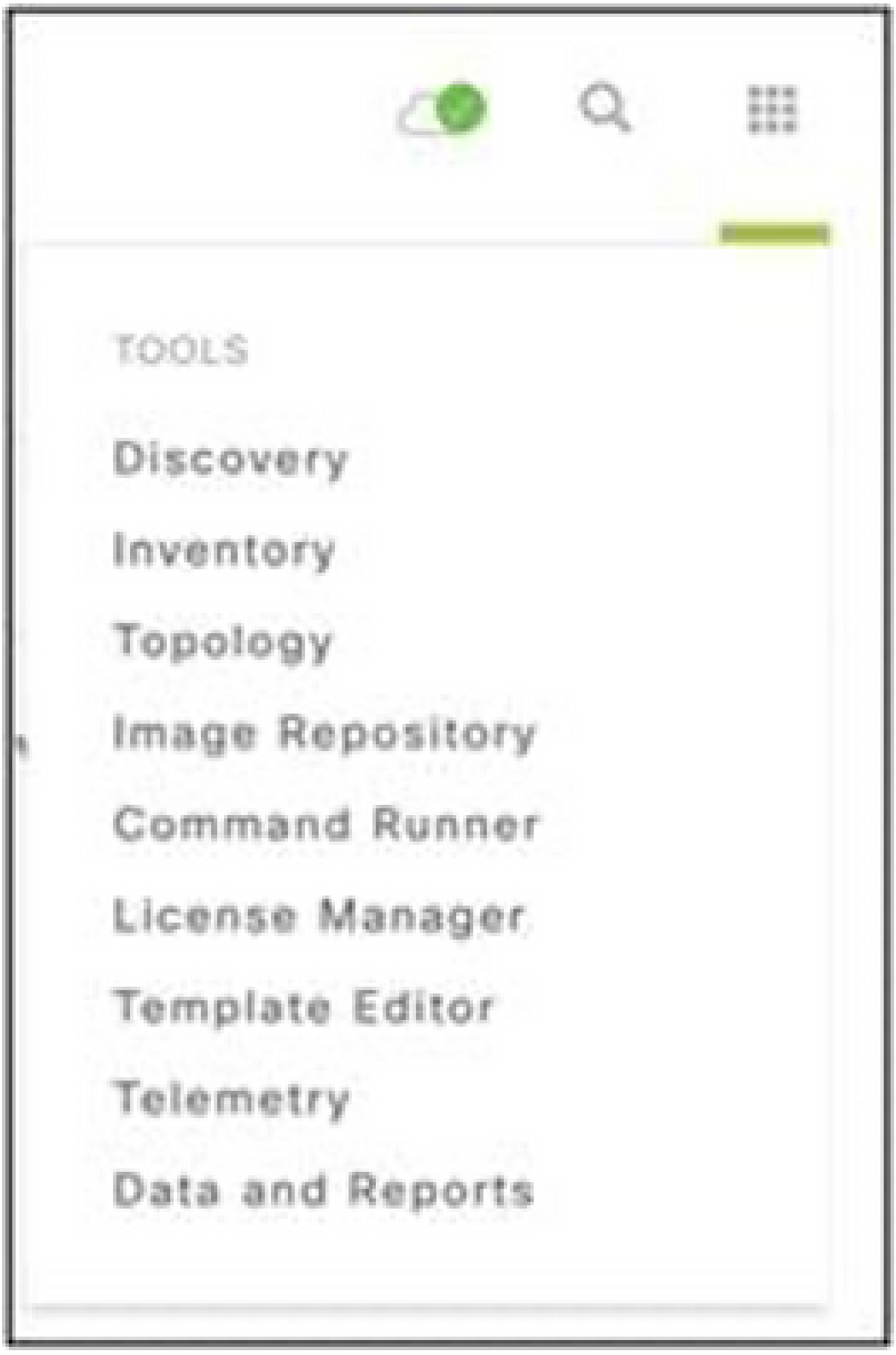
Guida alla configurazione di Cisco IOS® XE

Guida alla configurazione di AireOS Wireless Controller

Abilita impostazioni syslog livello informazioni

Per rendere visibile il livello Informazioni syslog, effettuare le seguenti operazioni:

1. Selezionare Strumenti>Telemetria.


TOOLS
Discovery
Inventory
Topology
Image Repository
Command Runner
License Manager
Template Editor
Telemetry
Data and Reports

Menu Strumenti

2. Selezionare ed espandere la visualizzazione Sito e selezionare un sito dalla gerarchia.

Vista della sede

3. Selezionare il sito desiderato e selezionare tutte le periferiche che utilizzano la casella di controllo Nome periferica.

4. Selezionare Visibilità ottimale dall'elenco a discesa Azioni.

Azioni

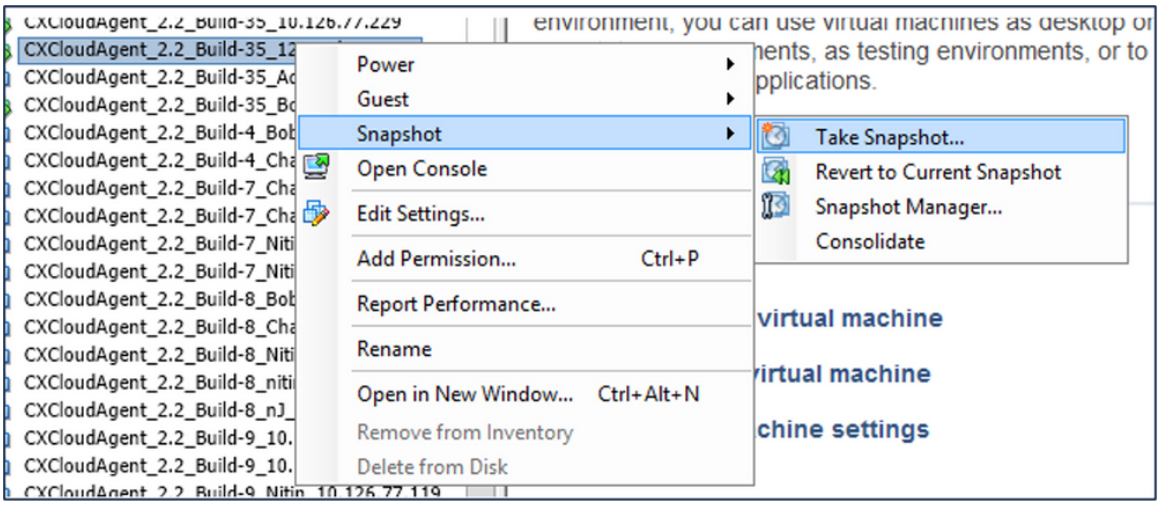
Backup e ripristino della VM cloud CX

Si consiglia di conservare lo stato e i dati di una VM agente cloud CX in un determinato point in time utilizzando la funzione di istantanea. Questa funzione facilita il ripristino della VM del cloud CX fino all'ora specifica in cui viene eseguita la copia istantanea.

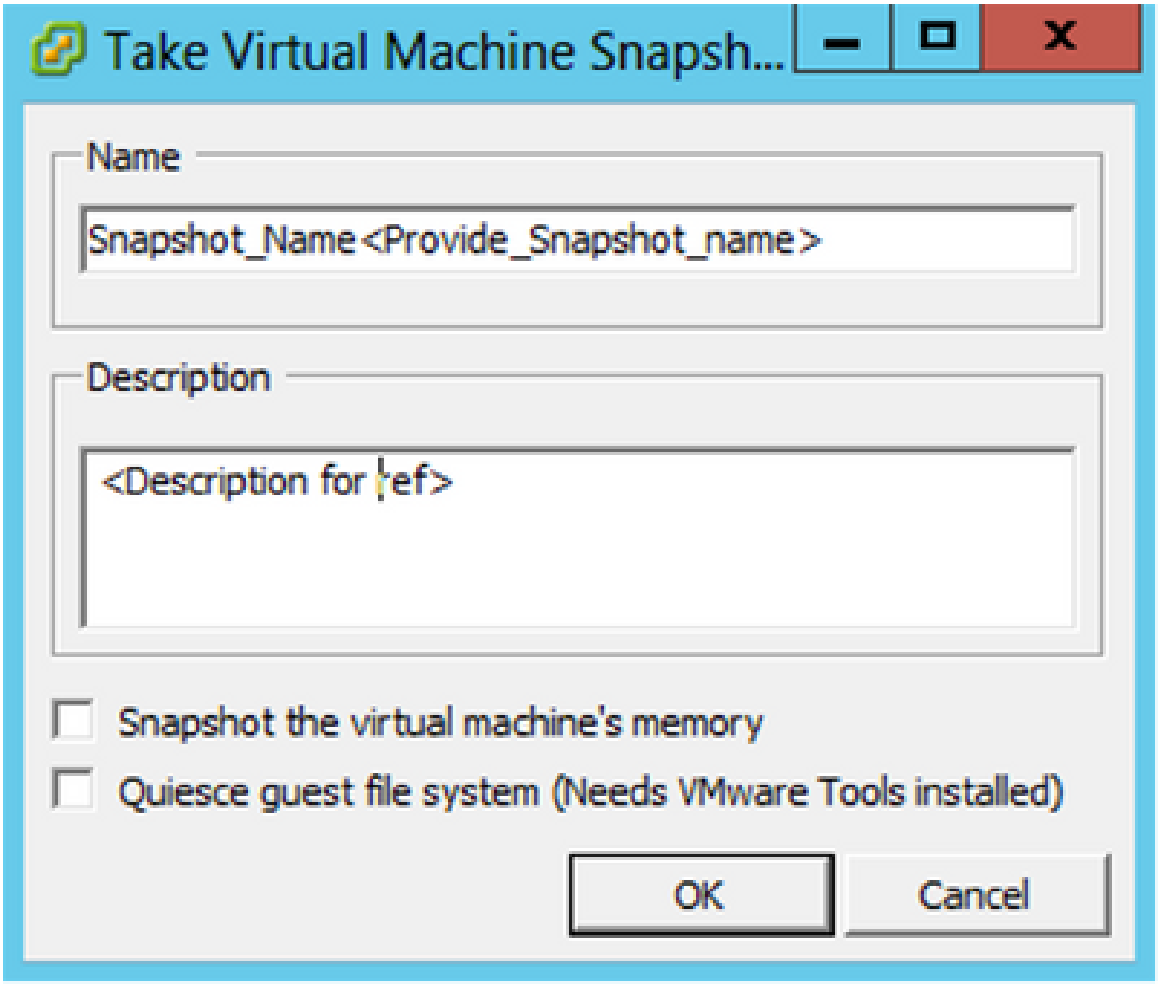
Backup

Per eseguire il backup della VM del cloud CX:

1. Fare clic con il pulsante destro del mouse sulla VM e selezionare Istantanea > Crea istantanea. Viene visualizzata la finestra Crea snapshot macchina virtuale.



Selezione della VM

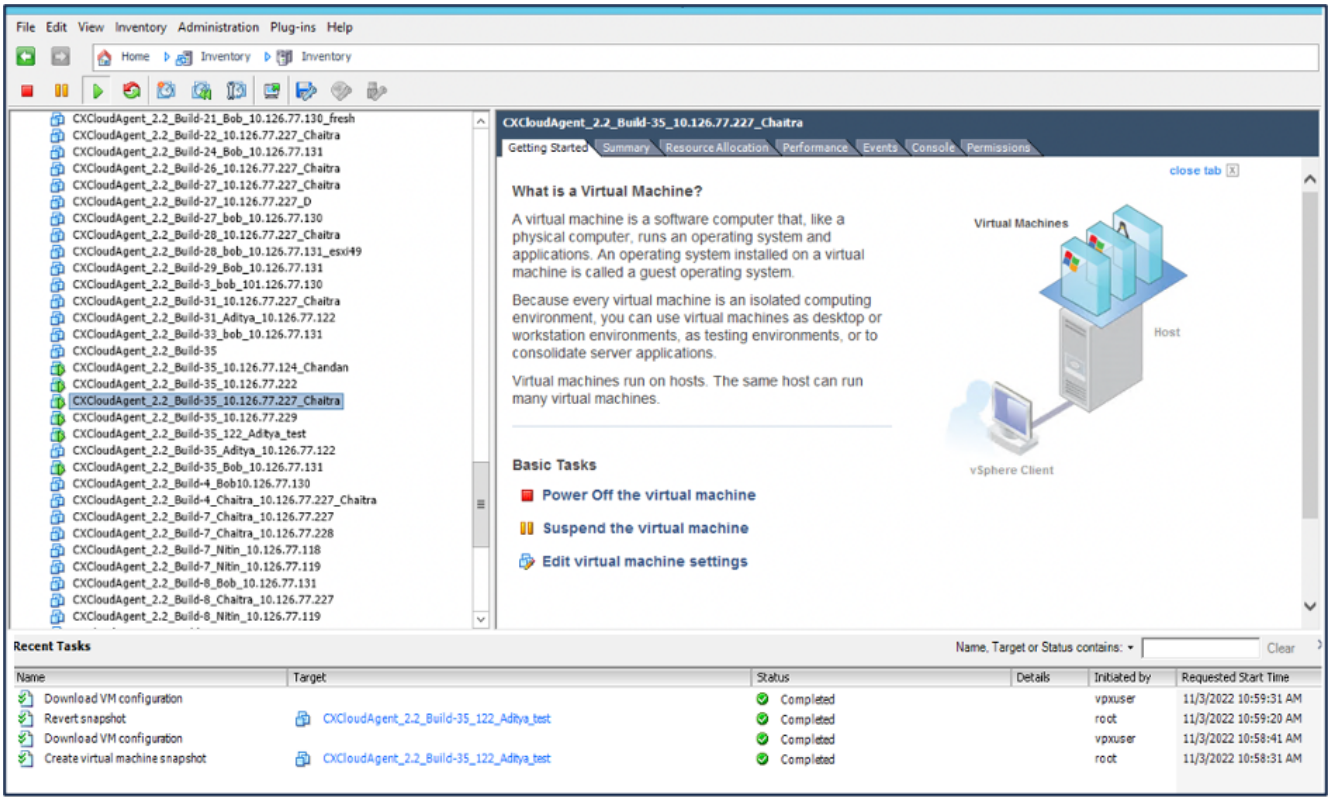


Crea snapshot macchina virtuale

2. Immettere Nome e Descrizione.

Nota: verificare che la casella di controllo Esegui snapshot della memoria della macchina virtuale sia deselezionata.

3. Fare clic su OK. Lo stato Crea snapshot macchina virtuale viene visualizzato come Completato nell'elenco Attività recenti.

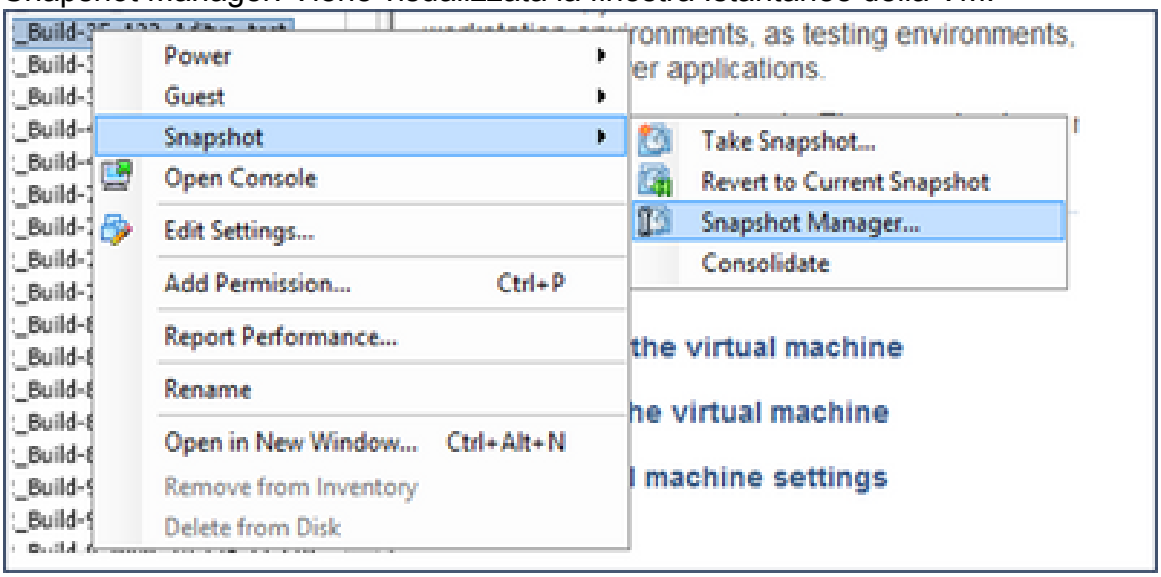


Attività recenti

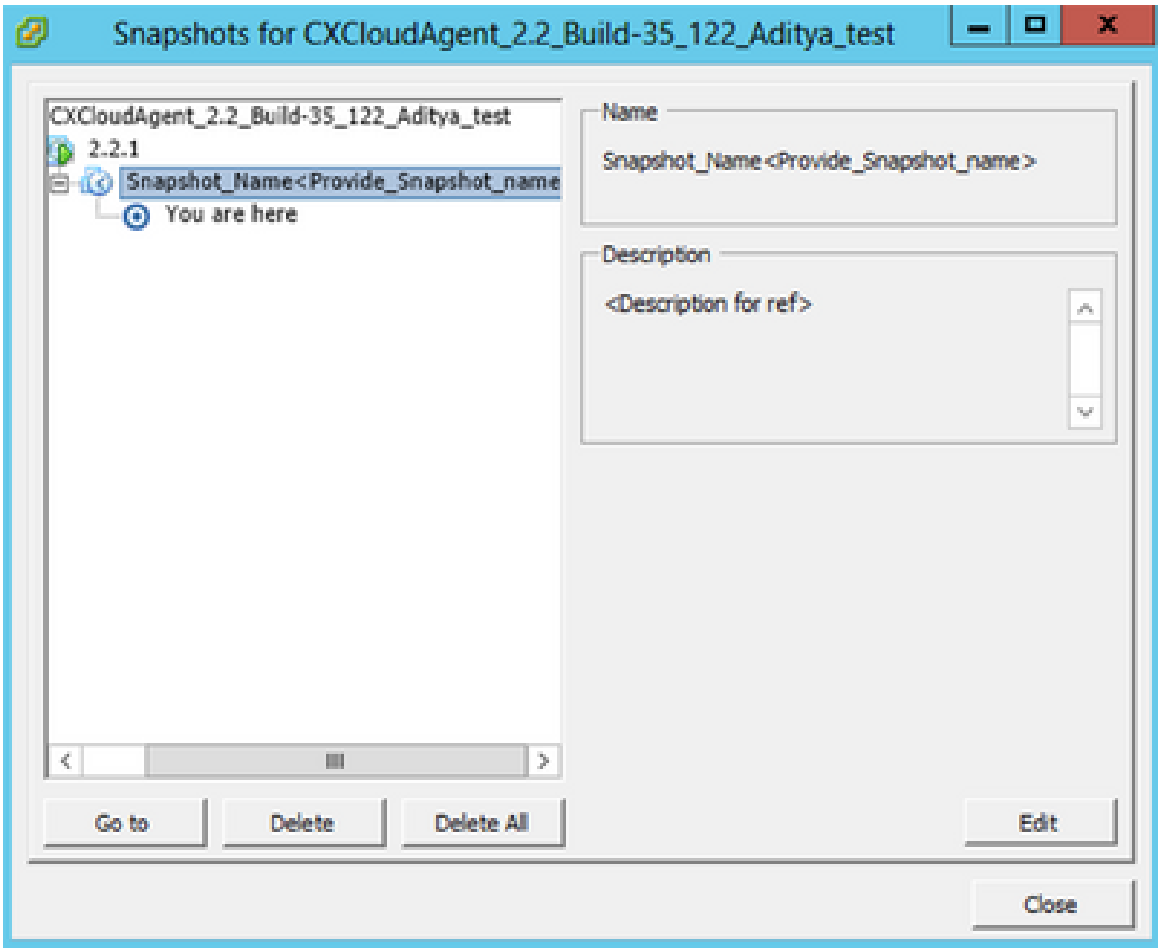
Ripristina

Per ripristinare la VM del cloud CX:

1. Fare clic con il pulsante destro del mouse sulla VM e selezionare Snapshot > Snapshot Manager. Viene visualizzata la finestra Istantanee della VM.

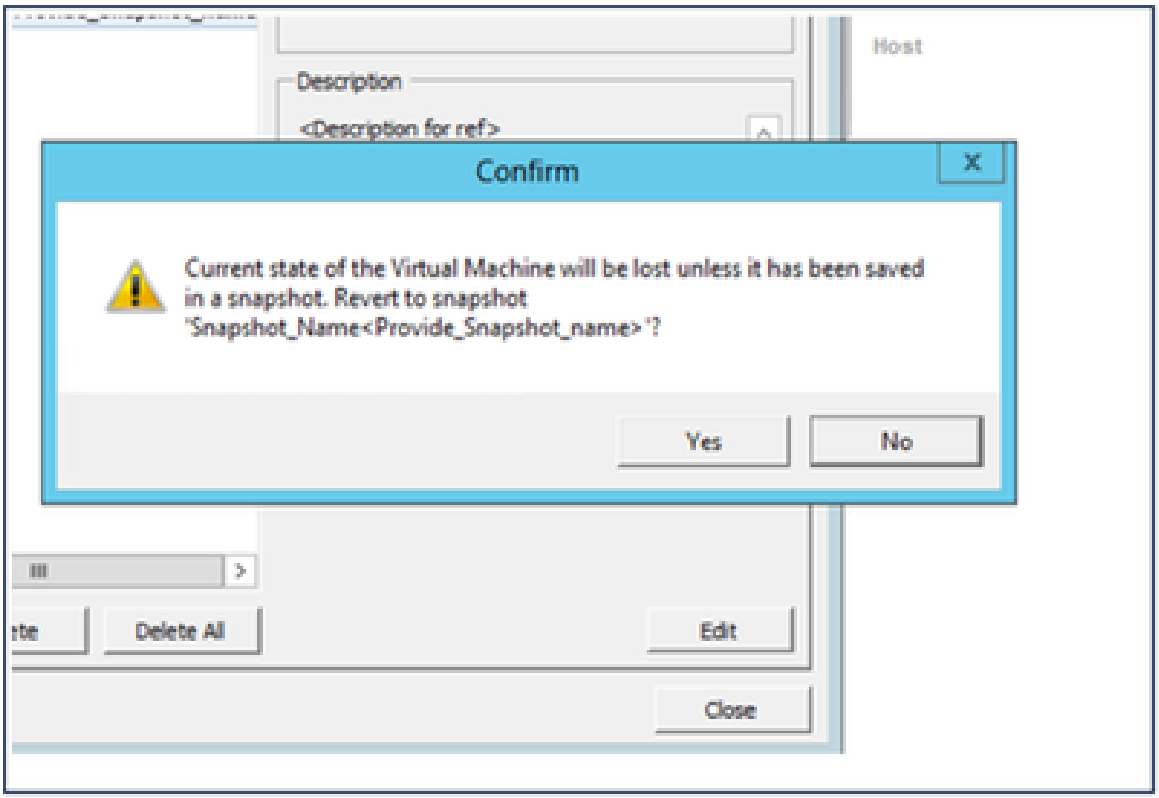


Finestra Seleziona VM



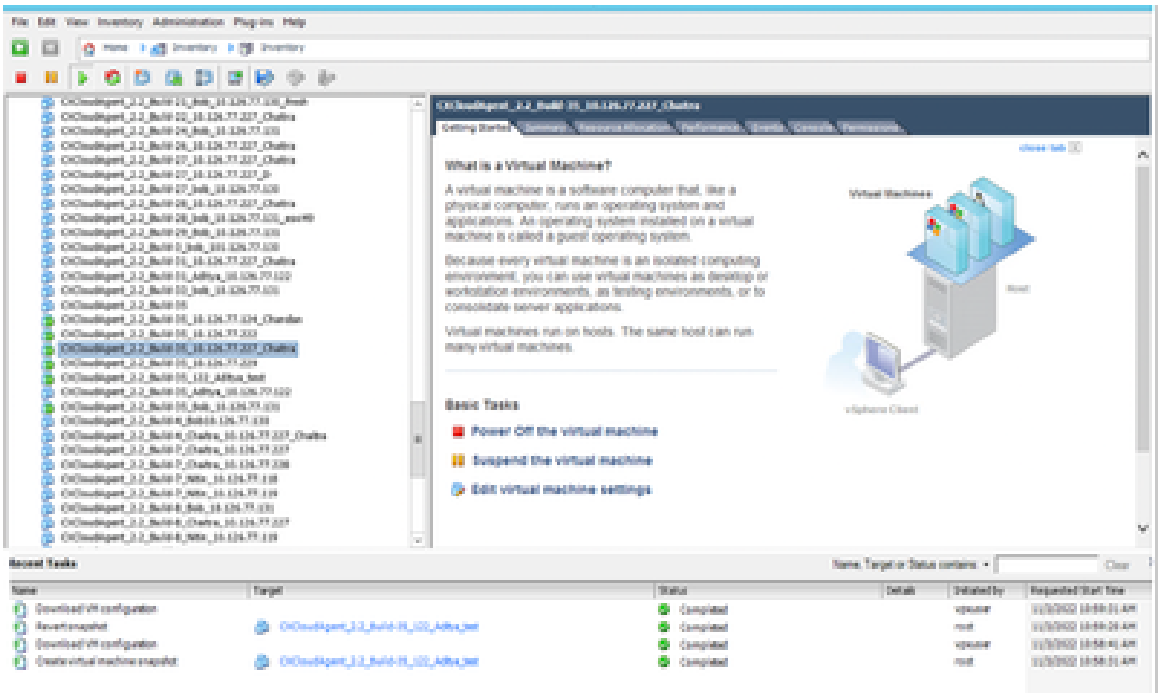
Finestra Snapshot

2. Fare clic su Vai a. Viene visualizzata la finestra Conferma.



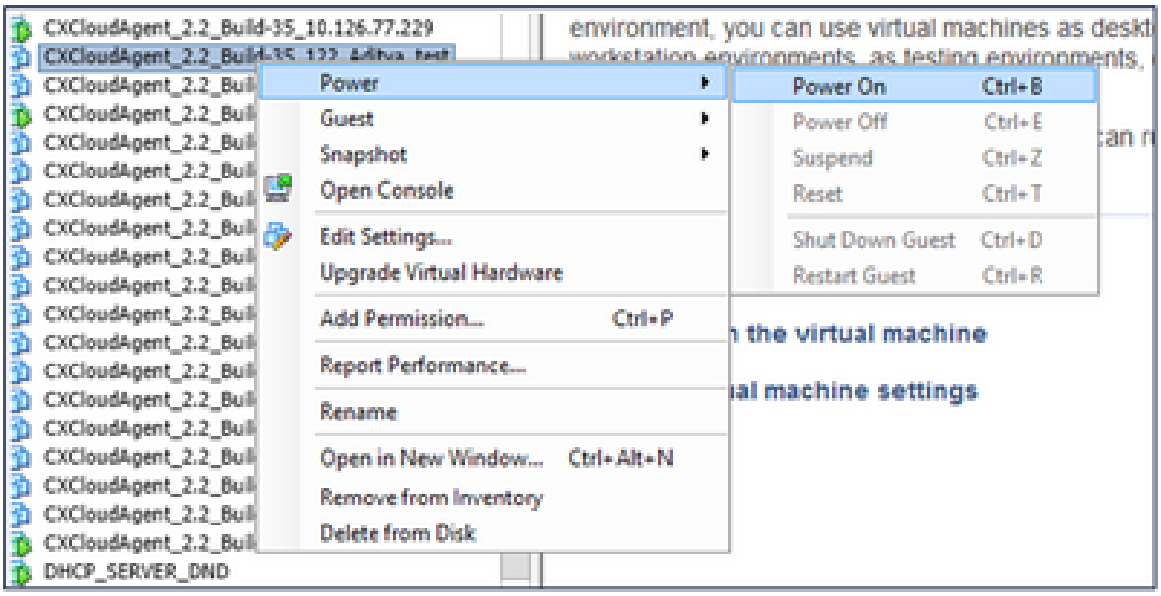
Finestra Conferma

3. Fare clic su Sì. Lo stato Ripristina snapshot viene visualizzato come Completato nell'elenco Attività recenti.



Attività recenti

4. Fare clic con il pulsante destro del mouse sulla VM e selezionare Accensione > Accendi per accendere la VM.



Sicurezza

CX Cloud Agent garantisce la sicurezza end-to-end. La connessione tra CX Cloud e CX Cloud Agent è protetta da TLS. L'utente SSH predefinito dell'agente cloud deve eseguire solo le operazioni di base.

Sicurezza fisica

Distribuire l'immagine OAV dell'agente cloud CX in un'azienda server VMware protetta. L'OVA viene condivisa in modo sicuro dal centro di download del software Cisco. Per il bootloader (modalità utente singolo) viene impostata una password univoca scelta casualmente. Gli utenti devono fare riferimento a queste domande frequenti per impostare la password del bootloader (modalità utente singolo).

Sicurezza dell'account

Durante la distribuzione, viene creato l'account utente cxcadmin. Gli utenti sono obbligati a impostare una password durante la configurazione iniziale. Le credenziali e gli utenti cxcadmin vengono utilizzati per accedere alle API dell'agente cloud CX e per connettersi all'accessorio tramite SSH.

gli utenti cxcadmin dispongono di un accesso limitato con il minor numero di privilegi. La password cxcadmin segue i criteri di protezione ed è sottoposta a hash unidirezionale con un periodo di scadenza di 90 giorni. Gli utenti cxcadmin possono creare un utente cxcroot utilizzando l'utilità denominata remoteaccount. Gli utenti cxcadmin possono ottenere i privilegi root.

Sicurezza della rete

È possibile accedere alla VM dell'agente cloud CX utilizzando SSH con le credenziali utente cxcadmin. Le porte in arrivo sono limitate a 22 (SSH), 514 (Syslog).

Autenticazione

Autenticazione basata su password: l'accessorio gestisce un singolo utente (cxcadmin) che consente all'utente di autenticarsi e comunicare con l'agente cloud CX.

- Azioni eseguibili sull'appliance con privilegi root tramite SSH.

gli utenti cxcadmin possono creare utenti cxcroot utilizzando un'utilità denominata remoteaccount. Questa utility visualizza una password crittografata RSA/ECB/PKCS1v1_5 che può essere decrittografata solo dal portale SWIM (modulo di richiesta DECRYPT). Solo il personale autorizzato può accedere a questo portale. Gli utenti di Cxcroot possono ottenere i privilegi di root utilizzando questa password decrittografata. La passphrase è valida solo per due giorni. Gli utenti cxcadmin devono ricreare l'account e ottenere la password dalla scadenza della password del post-portale SWIM.

Protezione avanzata

L'appliance CX Cloud Agent è conforme agli standard di protezione avanzata di Center of Internet Security.

Sicurezza dei dati

L'appliance CX Cloud Agent non memorizza le informazioni personali dei clienti. L'applicazione per le credenziali del dispositivo (in esecuzione come uno dei pod) archivia le credenziali del server crittografato all'interno del database protetto. I dati raccolti non vengono memorizzati in alcun modo all'interno dell'accessorio, se non temporaneamente durante l'elaborazione. I dati di telemetria vengono caricati in CX Cloud appena possibile dopo il completamento della raccolta e vengono immediatamente eliminati dallo storage locale dopo la conferma del corretto caricamento.

Trasmissione dati

Il pacchetto di registrazione contiene il certificato e le chiavi univoci richiesti per il dispositivo X.509 per stabilire una connessione sicura con Iot Core. Tramite tale agente viene stabilita una connessione protetta utilizzando il protocollo MQTT (Message Queuing Telemetry Transport) su TLS (Transport Layer Security) versione 1.2

Log e monitoraggio

I registri non contengono alcun tipo di dati PII (Personal Identifier Information). I registri di verifica acquisiscono tutte le azioni relative alla sicurezza eseguite sull'appliance CX Cloud Agent.

Comandi di telemetria Cisco

CX Cloud recupera la telemetria degli asset utilizzando le API e i comandi elencati nei comandi di telemetria Cisco. Questo documento classifica i comandi in base alla loro applicabilità all'inventario Cisco DNA Center, al Diagnostic Bridge, all'Intersight, alle informazioni sulla

conformità, ai guasti e a tutte le altre fonti di telemetria raccolte dall'agente cloud CX.

Le informazioni sensibili all'interno della telemetria degli asset vengono nascoste prima di essere trasmesse al cloud. L'agente cloud CX maschera i dati sensibili per tutte le risorse raccolte che inviano la telemetria direttamente all'agente cloud CX. ad esempio password, chiavi, stringhe della community, nomi utente e così via. I controller forniscono il masking dei dati per tutte le risorse gestite dai controller prima di trasferire queste informazioni all'agente cloud CX. In alcuni casi, la telemetria delle risorse gestite dai controller può essere ulteriormente anonimizzata. Per ulteriori informazioni sull'anonimizzazione della telemetria (ad esempio, la sezione Anonimizza dati della Cisco DNA Center Administrator Guide), consultare la documentazione di supporto del prodotto corrispondente.

Anche se l'elenco dei comandi di telemetria non può essere personalizzato e le regole di mascheramento dei dati non possono essere modificate, i clienti possono controllare gli accessi di telemetria degli asset a CX Cloud specificando le origini dati come indicato nella documentazione di supporto del prodotto per i dispositivi gestiti da controller o nella sezione Connessione delle origini dati di questo documento (per Altre risorse raccolte da CX Cloud Agent).

Riepilogo delle funzionalità di sicurezza

Funzionalità di sicurezza	Descrizione
Password del bootloader	Per il bootloader (modalità utente singolo) viene impostata una password univoca scelta casualmente. Gli utenti devono fare riferimento alle domande frequenti per impostare la password del bootloader (modalità utente singolo).
Accesso utente	SSH: ·Per accedere all'appliance con l'utente cxcadmin, occorre utilizzare le credenziali create durante l'installazione. · L'accesso all'accessorio tramite l'utente cxcroot richiede la decrittografia delle credenziali tramite il portale SWIM da parte di personale autorizzato.
Account utente	· cxcadmin: account utente predefinito creato; l'utente può eseguire i comandi dell'applicazione CX Cloud Agent utilizzando cxcli e dispone dei privilegi minimi sull'accessorio; l'utente cxcadmin e la relativa password crittografata vengono generati utilizzando cxcadmin user. · cxcroot: cxcadmin consente di creare l'utente utilizzando l'account remoto dell'utilità. L'utente può ottenere i privilegi root con questo account.
Policy della	·La password ha un hash unidirezionale che utilizza SHA-256 e viene

password di cxcadmin	memorizzata in modo sicuro. · Almeno otto (8) caratteri, contenenti tre di queste categorie: maiuscole, minuscole, numeri e caratteri speciali.
Policy della password cxcroot	·La password di cxcroot è RSA/ECB/PKCS1v1_5 ed è criptata ·La passphrase generata deve essere decriptata nel portale SWIM. · L'utente e la password cxcroot sono validi per due giorni e possono essere rigenerati utilizzando cxcadmin user.
Policy della password di accesso tramite SSH	· Un minimo di otto caratteri che contengono tre di queste categorie: maiuscole, minuscole, numeri e caratteri speciali. · Cinque tentativi di login non riusciti bloccano la scatola per 30 minuti; la password scade tra 90 giorni.
Porte	Porte in ingresso aperte - 514 (Syslog) e 22 (SSH)
Sicurezza dei dati	·Nessuna informazione dei clienti viene memorizzata. ·Nessun dato dei dispositivi viene memorizzato. ·Le credenziali del server Cisco DNA Center sono criptate e memorizzate nel database.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).